

Understanding NYDFS Cybersecurity Regulations in 2022: Why Regulatory Action is Key

Presented by:

Daniel B. Garrie Esq., Co-Founder and Senior Managing Partner, Law & Forensics, Neutral, Mediator, E-discovery Special Master, JAMS

Jeff Boogay, Partner, Mullen Coughlin LLC

Joseph Johnson, Chief Information Security Officer, Premise Health

Vlad Brodsky, OTC Markets Group - SVP, IT Operations, Infrastructure/CISO

Richard Borden, Wilkie Farr & Gallagher LLP – Counsel

(c) 2022 Lexeprint Inc. All Rights Reserved.

Speakers



Daniel B. Garrie, Esq.
Co-founder, Law & Forensics
Mediator, Arbitrator, and
eDiscovery Special Master, JAMS



Jeff Boogay
Partner
Mullen Coughlin LLC



Joey Johnson
Chief Information Security Officer
Premise Health



Vlad Brodsky
OTC Markets Group - SVP, IT
Operations, Infrastructure/CISO



Richard Borden
Wilkie Farr & Gallagher LLP –
Counsel

(c) 2022 Lexeprint Inc. All Rights Reserved.

Disclaimer



This is not legal advice, nor should it be considered legal advice.

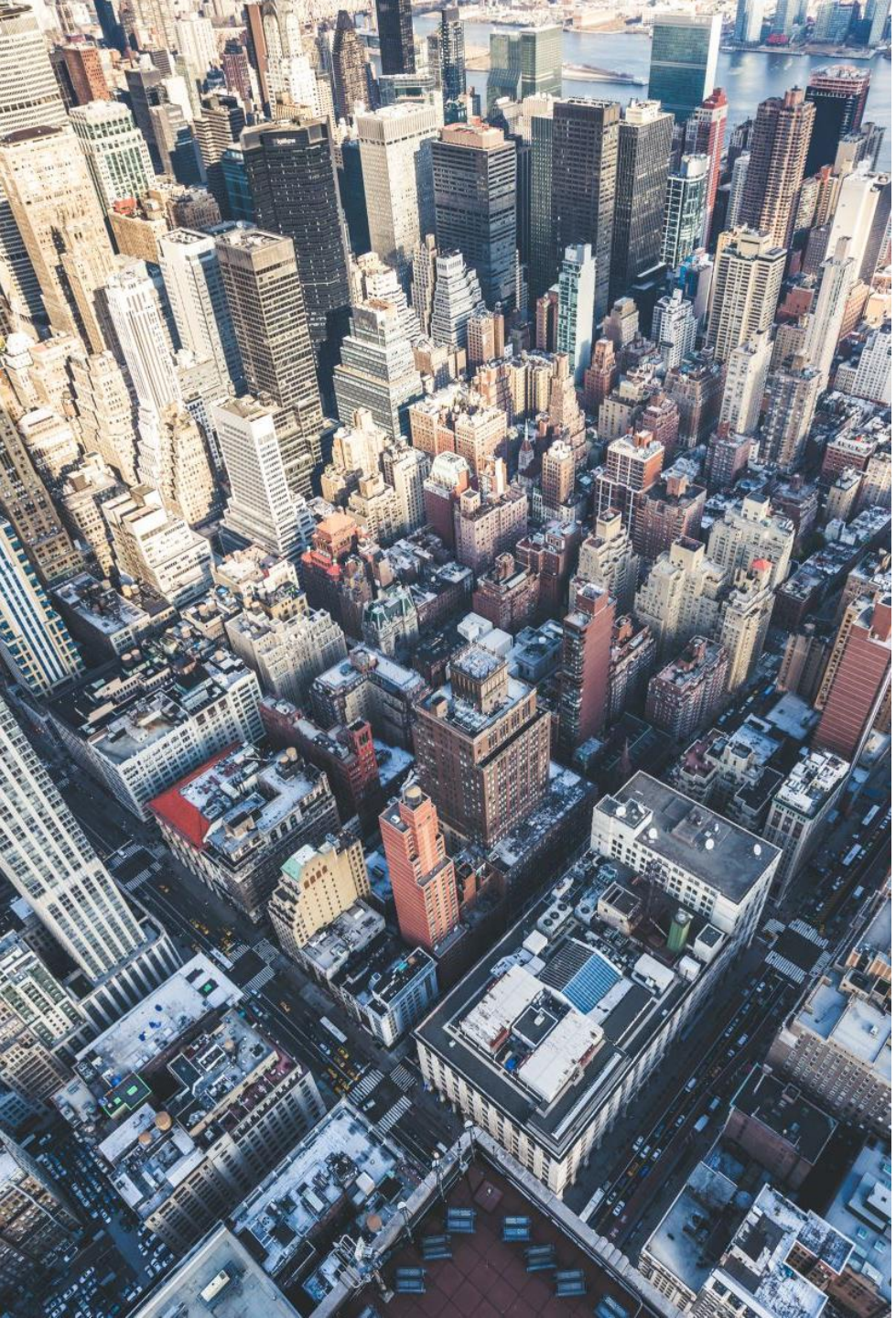


This presentation and the comments contained therein represent only the personal views of the participants, and do not reflect those of their employers or clients.



This presentation is offered for educational and informational uses only.

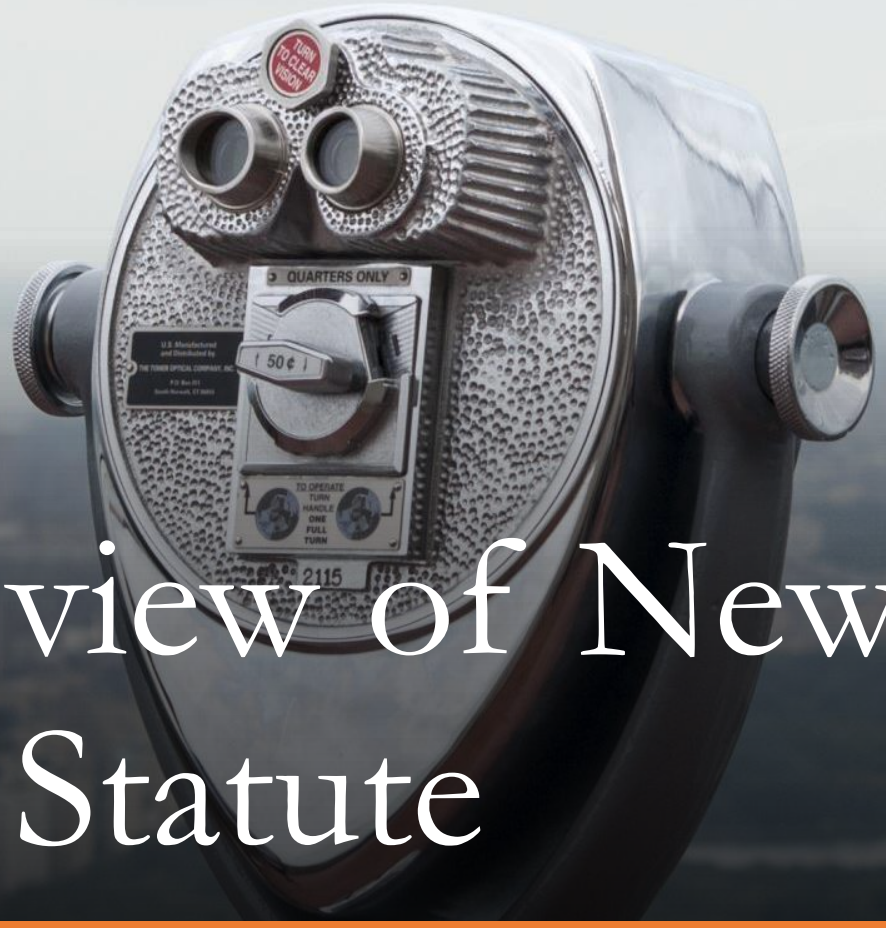
(c) 2022 Lexeprint Inc. All Rights Reserved.



Agenda

- Overview of New York DFS Statute
- Understanding the DFS Statute
- Risk Assessment
- Incident Response Plan

(c) 2022 Lexeprint Inc. All Rights Reserved.



Overview of New York DFS Statute

(c) 2022 Lexeprint Inc. All Rights Reserved.

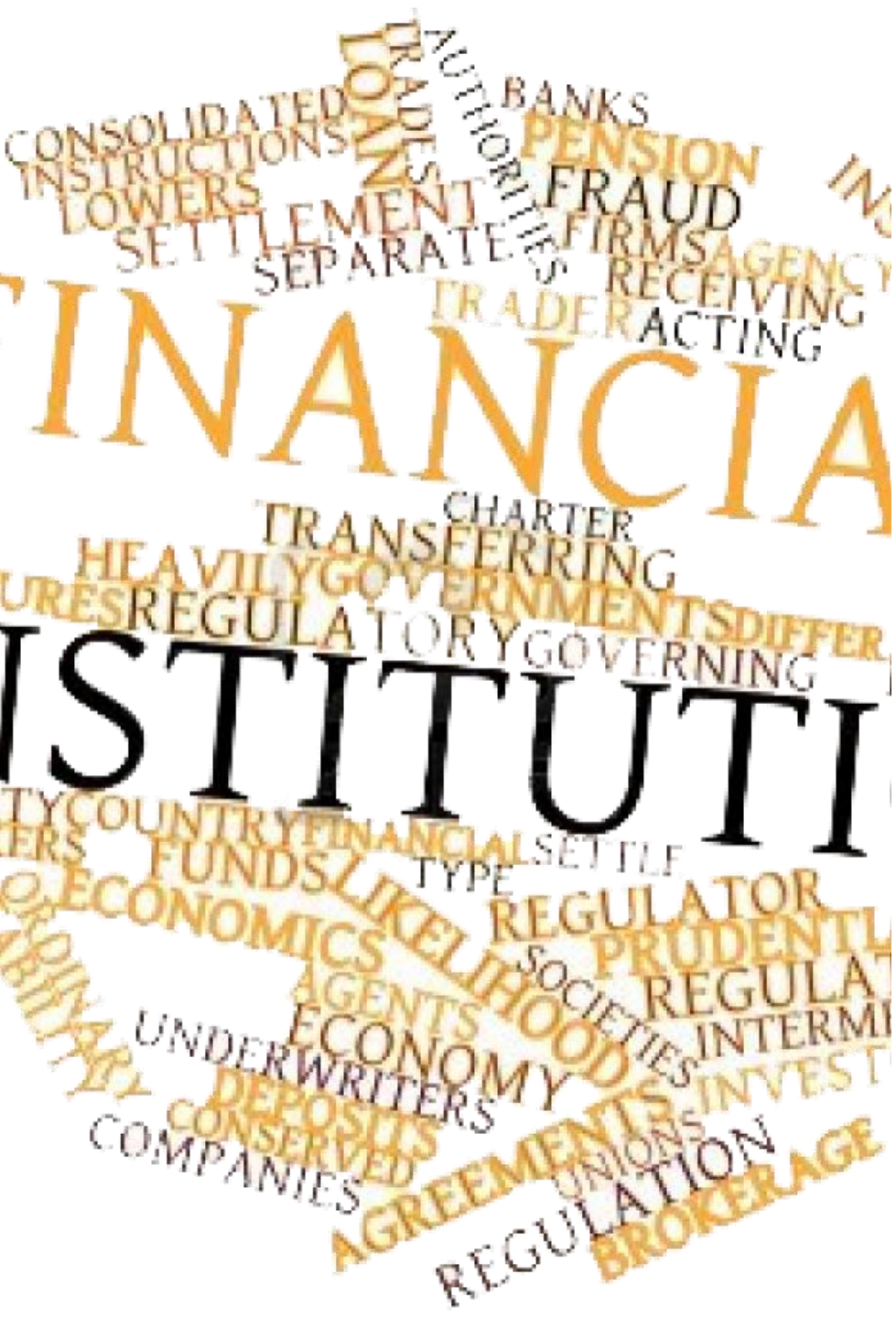


This Photo by Unknown Author is licensed under CC BY

NYDFS Cybersecurity Regulation

- The NYDFS Cybersecurity Regulation enforces cybersecurity guidelines on all covered financial institutions/entities through a four-step implementation process.
- The rules were released on February 16, 2017 and included 23 sections of guidelines to develop and effective cybersecurity measures.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Covered Cybersecurity Regulations

- Covered financial institutions that must follow the regulations include:
  - State-chartered banks
  - Licensed lenders
  - Private bankers
  - Foreign banks licensed to operate in New York
  - Mortgage and insurance companies
  - Service providers

(c) 2022 Lexeprint Inc. All Rights Reserved.



Covered Entities

- Covered Entities are defined as:
  - "[A]ny Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law."
- Exemptions:
  - Small covered entities are exempt from some requirements, including designating a CISO and performing vulnerability assessments each year. - 23 NYCRR 500.01(c)

(c) 2022 Lexeprint Inc. All Rights Reserved.



Why does the NYDFS Regulation matter?

- Studies show that the value at risk globally from cybercrime is estimated at $5.2 trillion dollars from 2019 to 2023.
- The bill is the "first-in-the-nation" regulation concerning cybersecurity and goes beyond other cybersecurity regulations, including the Graham Leach Bliley Act.
- The regulation covers information and systems that do not include, store, process or maintain PII.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Why does the NYDFS Regulation matter?

- The regulation requires new compliance processes and is built around the Risk Assessment to ensure personal data is protected.
- The regulation has forced many covered entities to modify and expand existing protocols to meet regulatory requirements.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Understanding the DFS Statute

(c) 2022 Lexeprint Inc. All Rights Reserved.



Overview of the DFS Regulation – 23 NYCRR 500

- A regulatory system of minimum standards is necessary to promote the protection of customer information and information technology systems.
- The plan includes the following requirements:
  - Cybersecurity program
  - Cybersecurity policy
  - Chief Information Security Officer (CISO)

(c) 2022 Lexeprint Inc. All Rights Reserved.

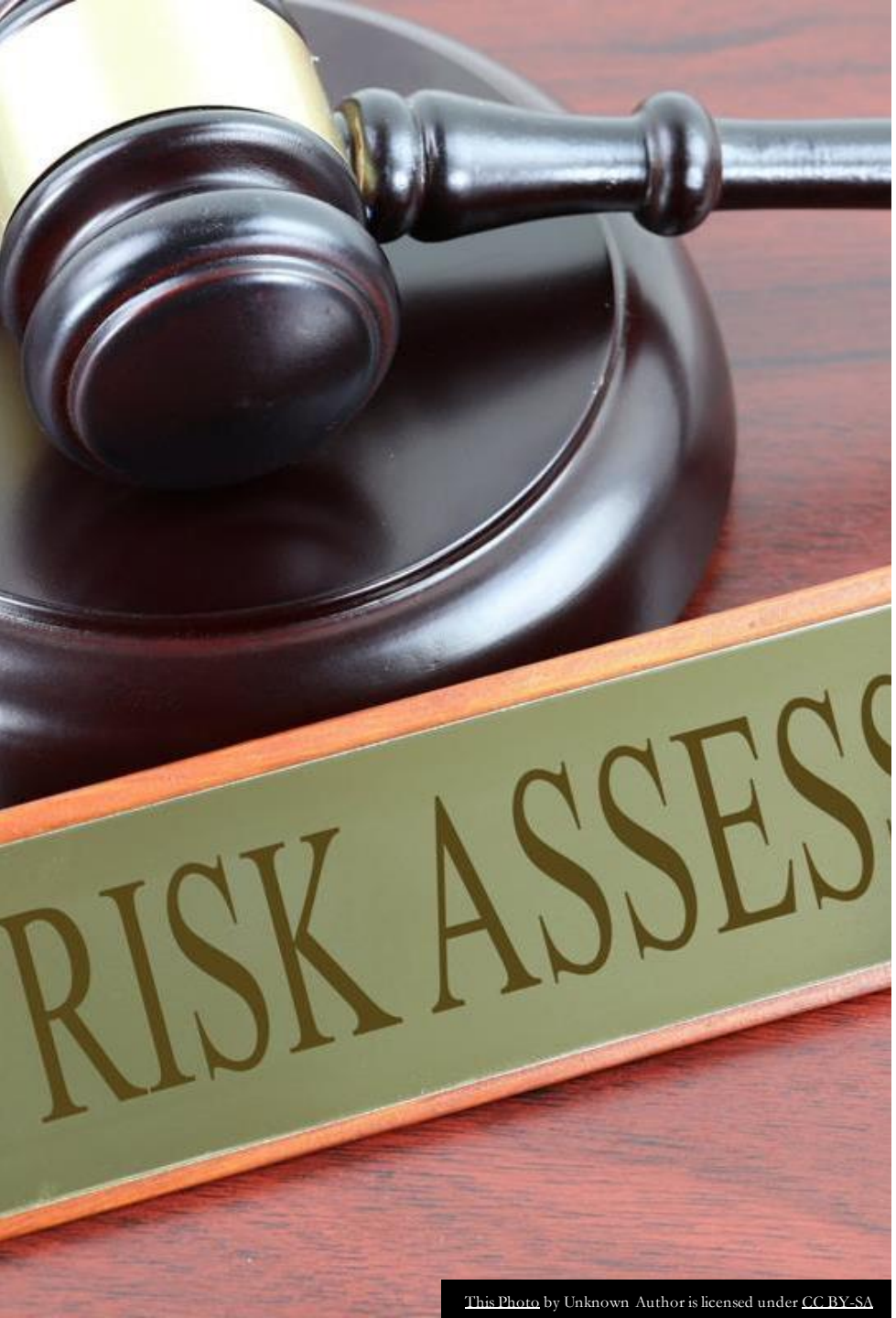


This Photo by Unknown Author is licensed under CC BY-SA

Required Policies and Procedures by DFS Statute

- Risk Assessment (Basis for other policies and procedures/actions)
- Written Cybersecurity Policy
- 3rd Party Information Security Policy
- Limitations on Data Retention
- Training & Monitoring
- Incident & Response Plan
- Application Security

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA

Risk Assessment Requirement 23 NYCRR 500.09(b)

- Risk Assessment is the backbone of the cybersecurity program.
  - Policies and procedures shall include:
    - (1) criteria for the evaluation and categorization of identified risks/threats facing the Covered Entity;
    - (2) criteria for the assessment of the confidentiality, integrity, security & availability of the Covered Entity's Information Systems; and
    - (3) requirements describing how identified risks will be mitigated based on the Risk Assessment and how the cybersecurity program will address them.

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY

Cybersecurity Program 23 NYCRR 500.02

- Each company "shall establish and maintain a cybersecurity program designed to ensure the confidentiality, integrity and availability of the Covered Entity's Information Systems."
- The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform core cybersecurity functions.

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY

Cybersecurity Program 23 NYCRR 500.02

- The written cybersecurity policy mandated by the Regulation must be approved by a "Senior Officer" and requires inclusion of 14 key areas.
- Senior Officers are responsible for the management, operations, security, information systems, compliance and/or risk of a Covered Entity.
- The policy must ultimately be based on the Risk Assessment.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Required Actions

(c) 2022 Lexeprint Inc. All Rights Reserved.



Required Actions By DFS Statute

- Establishment of Qualified Chief Information Security Officer ("CISO")
- Testing Vulnerability Assessments Encryption of Data at Rest and in Transit
- Preservation of Audit Data (to reconstruct transactions and cyber events)
- Data Minimization
- Notices to Superintendent

(c) 2022 Lexeprint Inc. All Rights Reserved.



Chief Information Security Officer (CISO) 23 NYCRR 500.04

- Covered Entities will have to designate a "qualified individual" to serve as the CISO who will be "responsible for overseeing and implementing the [company's] cybersecurity program and enforcing its cybersecurity policy."
- Covered Entities must have cybersecurity personnel sufficient to manage the cybersecurity risks and perform the core functions.
- The CISO will be responsible for producing reports at least annually.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Incident Response Plan

(c) 2022 Lexeprint Inc. All Rights Reserved.



Incident Response Plan and Notice 23 NYCRR 500.16, 500.17

- As part of the cybersecurity program, the Covered Entity must establish an incidence response plan to recover from a cybersecurity breach/attempted breach.
- The entity must provide a notice to the Superintendent within **72** hours from a determination that a cyber incident has occurred and has "a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity."

(c) 2022 Lexeprint Inc. All Rights Reserved.



Incident Response Plan and Notice 23 NYCRR 500.16, 500.17

- The response plan should include:
  - "The internal processes for responding to a cybersecurity event;
  - The goals of the incident response plan;
  - The definition of clear roles, responsibilities and levels of decision-making authority;
  - External and internal communications and information sharing…

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA

Incident Response Plan and Notice 23 NYCRR 500.16, 500.17

- It should also include:
  - Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
  - Documentation and reporting regarding cybersecurity events and related incident response activities; and
  - The evaluation and revision as necessary of the incident response plan following a cybersecurity event."

(c) 2022 Lexeprint Inc. All Rights Reserved.



Questions?

(c) 2022 Lexeprint Inc. All Rights Reserved.

Contact Us



Daniel Garrie
Email: daniel@lawandforensics.com
URL: www.lawandforensics.com



Jeff Boogay
Email: jboogay@mullen.law
URL: https://www.mullen.law/



Richard Borden
Email: rborden@willkie.com
URL: https://www.willkie.com



Joseph Johnson
Email: Joey.johnson@premisehealth.com



Vlad Brodsky
E: vlad@otcmarkets.com
URL: https://www.otcmarkets.com/

(c) 2022 Lexeprint Inc. All Rights Reserved.



Daniel B. Garrie, Esq.
Law & Forensics LLC – Co-Founder
JAMS – Special Master, Neutral, Arbitrator
Contact:
W: (855) 529-2466
E: daniel@lawandforensics.com
URL: https://www.lawandforensics.com/

LAW & FORENSICS
A Global Legal Engineering Firm

B.A., Computer Science, Brandeis Uni.
M.A., Computer Science Brandies Uni.
J.D., Rutgers School of Law

Daniel Garrie, Esq. is the Co-Founder of Law & Forensics LLC, where he heads the Computer Forensics and digital discovery Cybers ecurity teams. Daniel has been a dominant voice in the computer forensic and cybersecurity space for the past 20 years, as an attorney and technologist. He is an adjunct professor at Harvard for Computer Forensics and prior to Law & Forensics, he successfully built and sold several technology start-up companies.

Since co-founding Law & Forensics LLC in 2008, Daniel has built it into one of the leading boutique cybersecurity forensic engin eering firms in the industry. He is a mediator, arbitrator, and e-discovery special master for JAMS and is a partner and head of the Cybersecurity at Zeichner, Ellman & Krause LLP. Daniel has both a Bachelor's and a Master's degree in computer science from Brandeis University, as well as a J.D. from Rutgers Law School.

Daniel has led cyber and forensic teams in some of the most visible and sensitive cyber incidents in the United States. He an d his team have worked for two of the top five banks in the globe, and dozens of the largest private and public companies in the world. In addition, Daniel has been aw arded several patents for advanced cybersecurity and forensic platform he built with his team that is currently used in the industry, TableTop.AI, CustodyTrack. IO, and Forensic Scan.

Daniel is also well-published in the cybersecurity space and has authored more than 200 articles and books. His work is cited by Black's Law Dictionary 10th Ed. In defining the terms "software", "internet", and "algorithm." Lastly, he has been recognized by several United States Supreme C ourt Justices for his legal scholarship and is a trusted source and thought leader for cybersecurity articles and opinions, being cited over 500 times to date.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Jeff Boogay
Mullen Coughlin LLC - Partner
Contact:
E: jboogay@mullen.law
W: (267) 930-4784
URL: https://www.mullen.law/

MULLEN COUGHLIN

Jeff Boogay is a Partner at Mullen Coughlin LLC. Mr. Boogay assists clients in both preparation for and response to data security events and regulatory investigations and inquiries.

After a data security event has occurred, Mr. Boogay assists clients in addressing crucial points of fact and law, including: determining the nature and scope of the intrusion; identifying the affected individuals and types of information involved; determining what state, federal and foreign laws govern the client's notice of the incident; and preparing legally compliant notices to affected individuals and appropriate regulators, where required.

Prior to employment with Mullen Coughlin, Mr. Boogay worked for a large international firm where he litigated complex civil cases including allegations of violations of state unfair trade practice statutes.

Mr. Boogay is also a former Assistant District Attorney who worked closely with law enforcement and crime victims to investigate, prepare and litigate criminal cases, and draws on this experience to assist clients.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Joseph Johnson
Premise Health - Chief Information Security Officer
Contact:
E: Joey.johnson@premisehealth.com
URL: www.linkedin.com/in/joey-johnson-6453999/

Premise Health™
Keep your edge.

Joey Johnson is Chief Information Security Officer at Premise Health, provider of large employer sponsor health and wellness centers for employees. Joey is responsible for leading all organizational efforts related to security operations and engineering, information technology and security compliance, identity access management, policy development, security audit, and vendor risk management to meet challenging security and compliance demands. In his six years with Premise Health, Joey has been instrumental in implementing a proactive security and risk management environment focused organizational risk awareness that is transformative in the healthcare industry. He successfully launched a cutting-edge vendor and business associate maturity development program that dynamically empowered business partners of various scales and complexity to meet challenging security and compliance demands. Additionally, he has worked to develop a team driven by passion in security, with a focus on empowering and fostering women in the security field. In 2016 Joey was presented CISO of the Year award by the Nashville Technology Council.

Prior to joining Premise Health, Joey was the Chief Security Officer for the United States Department of Commerce, Office of Computer Services. He has over 15 years of experience in the cyber-security industry including leadership roles in both the public and private sectors, with a focus on organizations in the federal government, information technology, healthcare, and transportation industries. Outside of Premise Health Joey maintains an active leadership presence in the healthcare cyber-security industry participating in numerous steering and advisory committees with the National Healthcare Information Sharing & Analysis Center (NH-ISAC), various threat intelligence and sharing groups, security news groups, and private/public sector partnerships. He serves on the Editorial Board for the Journal of Law and Cyberwarfare helping to shape the future national and international regulatory landscape around cybersecurity, and also works as a senior advisory member on the E-Health Initiative Federal Executive Advisory Board on Privacy & Security. Joey additionally works as a technical advisor with various security & technology investment organizations and product companies, as well as frequently serving as a speaker at numerous security industry events.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Vlad Brodsky
OTC Markets Group - SVP, IT Operations, Infrastructure/CISO
Contact:
W: (212) 896-4464
E: vlad@otcmarkets.com
URL: https://www.otcmarkets.com/

Vlad Brodsky is currently the SVP of IT Operations and Infrastructure and Chief Information Security Officer at OTC Markets Group, a regulated publicly traded financial institution that operates the world's largest electronic marketplace for OTC-traded equities. Vlad's responsibilities include leading the firm's information security strategy, program, and processes. In his four years with OTC Markets Group, Vlad has been instrumental in creating a risk-based information security program that is designed to satisfy business and regulatory requirements.

Vlad has extensive expertise in IT Infrastructure Management, Information Security, and Risk Management. Prior to OTC Markets Group, Vlad worked as a Chief Security Officer for Innovest Systems, a SaaS provider in the Trust Accounting and Wealth Management space, where he was responsible for all Information Security.
Vlad has a Bachelor's degree in Computer Science from Brandeis University, an MBA in Finance and Management from NYU Leonard N. Stern School of Business and holds the CISSP, CRISC, PMP, and FINRA Series 99 certifications. He is also member of the board at New York Metro Infragard – a proactive collaboration between the FBI and the private sector to protect our nation's Critical Infrastructure.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Richard Borden
Wilkie Farr & Gallagher LLP – Counsel
Contact:
Email: rborden@willkie.com
Phone: (212) 728-3872
URL: https://www.willkie.com

WILLKIE
WILLKIE FARR & GALLAGHER LLP

Richard M. Borden is counsel in the Corporate & Financial Services Department and Cybersecurity and Privacy practice group where he focuses on intersecting areas such as technology transactions, cybersecurity and privacy risk management, Fintech and Insurtech.

Rick is at the forefront of cybersecurity and privacy issues, advising on big data governance and the Internet of Things, cybersecurity risk management, and technology sourcing and transactions. Rick translates the often complicated language of technology, cybersecurity, privacy, risk and compliance to assure that it's understood from both a legal and business perspective. His experience on both the customer and vendor side of matters enables him to advise general counsel, C-Suite executives and boards of directors on how to understand potential risks and how to respond should they suffer an incident. Mr .Borden also interfaces with technology departments, advising them on how technology tools and programs may expose companies to risk.

Rick regularly advises clients on data compliance programs, audits and responses to government compliance reviews, privacy policies, data sharing and the collection and use of employee and consumer personal data. He also works with clients to develop bring your own device (BYOD) and mobile computing policies and provides privacy and data protection legal analysis and compliance counseling.

Rick's significant experience across IT and legal sectors enables him to identify risk in light of process, policy and technology, and to effectively communicate with his clients, aligning strategy with their risk management tolerances. He also advises clients on cyber and privacy policies, best practices, reporting, auditing and review, and has extensive experience in regulatory investigations and compliance counseling, data breach insurance policies and claims, corporate risk and reporting, and post-breach penalties and audits.

EXPLORE MORE

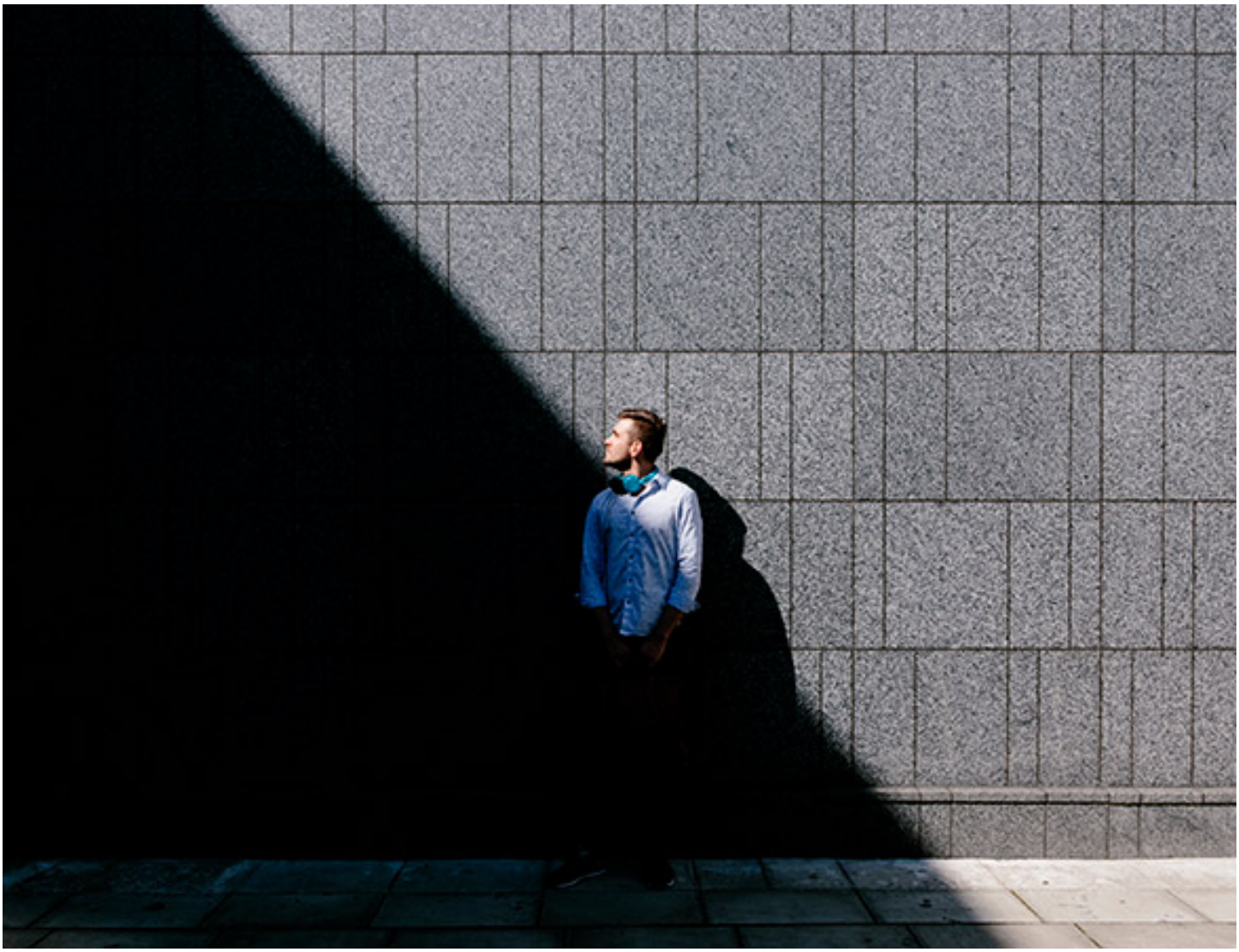
Overview

Cyber Threat Intelligence Report Volume 2

Cyber Threat Intelligence Report Volume 1

Volume 1

JULY 15, 2021



networks, it's challenging for OT and Industrial Control Systems (ICS) security professionals to keep pace with security demands.

Recent incidents and the large-scale disruptions and cost of ransomware operations illustrate the growing impact of cyber threat activity on enterprise risk across all industry segments. This risk is increasingly difficult to control and mitigate across both IT and OT environments.

While running industrial systems is eased by virtualization in the cloud and the advance of internet-connected devices, these technologies are also introducing new vulnerabilities and risks. In particular, edge devices, such as Internet of Things (IoT) objects, switches and routers to control data flowing in and out of the organization. Bordering IT and OT environments, they are critical to OT security and breaches can provide direct access into OT environments, completely bypassing IT networks.

Security leaders must demonstrate to the C-suite and the board that they understand the importance of both the continuity of operations and working in partnership with the whole business to effectively manage risk.

Our cyber threat intelligence and incident response analysts have gained first-hand visibility into the tactics, techniques and procedures (TTPs) employed by some of the most sophisticated cyber adversaries. This report reflects our analysis during the first half of calendar year 2021.

Key trends

Accenture analysis in the first half of 2021 identified four trends affecting the IT and OT landscape:



Ransomware actors test new extortion methods

Ransomware actors are expanding data leak extortion and devising new methods to pressure victims. Response options are becoming more complicated.

- **Targets are shifting:** The first months of 2021 targeted critical infrastructure and upstream

Organizations should focus on preparation, prevention and pre-encryption defenses.



Cobalt Strike is on the rise

The current high-profile success of Cobalt Strike abuse means the tool's popularity is growing—a trend that will almost certainly continue through 2021.

- **Cobalt Strike is proliferating:** Although in use for more than a decade, the number of Cobalt Strike-enabled attacks reportedly increased by 163% between 2019 and 2020.
- **Attack tools are evolving:** Threat actors are evolving their own custom loaders to deliver Cobalt Strike—such as facilitating the SolarWinds campaign.
- **Malware is merging:** For the first time, Accenture CTI has identified overlaps between the infrastructure of the information-stealing malware EvilGrab and Cobalt Strike Beacon in early 2021.

Organizations need to adopt new defensive tools that can counter this growing threat to penetration testing in critical production environments.

Commodity malware can invade OT from IT space

High-volume crimeware is a danger at the endpoint, enabling further intrusions within a victim network that can threaten both IT and OT systems.

- First-stage commodity malware enables the deployment of further malware at the endpoint.
- Second-stage commodity malware, or pseudo-malware such as pirated and abused Cobalt Strike instances, follow-on malware increases the risk of an infection spreading throughout an organization's infrastructure and even to OT assets if configured for that purpose.

vulnerability in the widely used Accellion File Transfer Appliance (FTA). Hades ransomware actors also gained traction in early 2021 and demonstrated their ability to bypass Endpoint Detection and Response tools[1] and reach edge devices and OT networks.

- **Information is easy to buy and even easier to use:** Accenture CTI observed a slight but noticeable increase in threat actors selling malware logs, which constitute data derived from information stealer malware.

Organizations need to share information among defenders to understand, prevent, identify and respond to threat activity.

Source:

[1] Welling, Eric, "It's getting hot in here! Unknown threat group using Hades ransomware to turn up the heat on their victims," Accenture, March 26, 2021. Read blog.

EXPLORE MORE

Overview

Cyber Threat Intelligence Report Volume 2

Cyber Threat Intelligence Report Volume 1

JAYSON JEAN
Senior Manager – Accenture Security

MORE ON THIS TOPIC



Security

The state of cybersecurity resilience 2021



Security

Ransomware response and recovery

Related capabilities



Cloud Security

The importance of cloud security

scalable and cost...

Stay in the know with our newsletter

SUBSCRIBE

ata across the organization

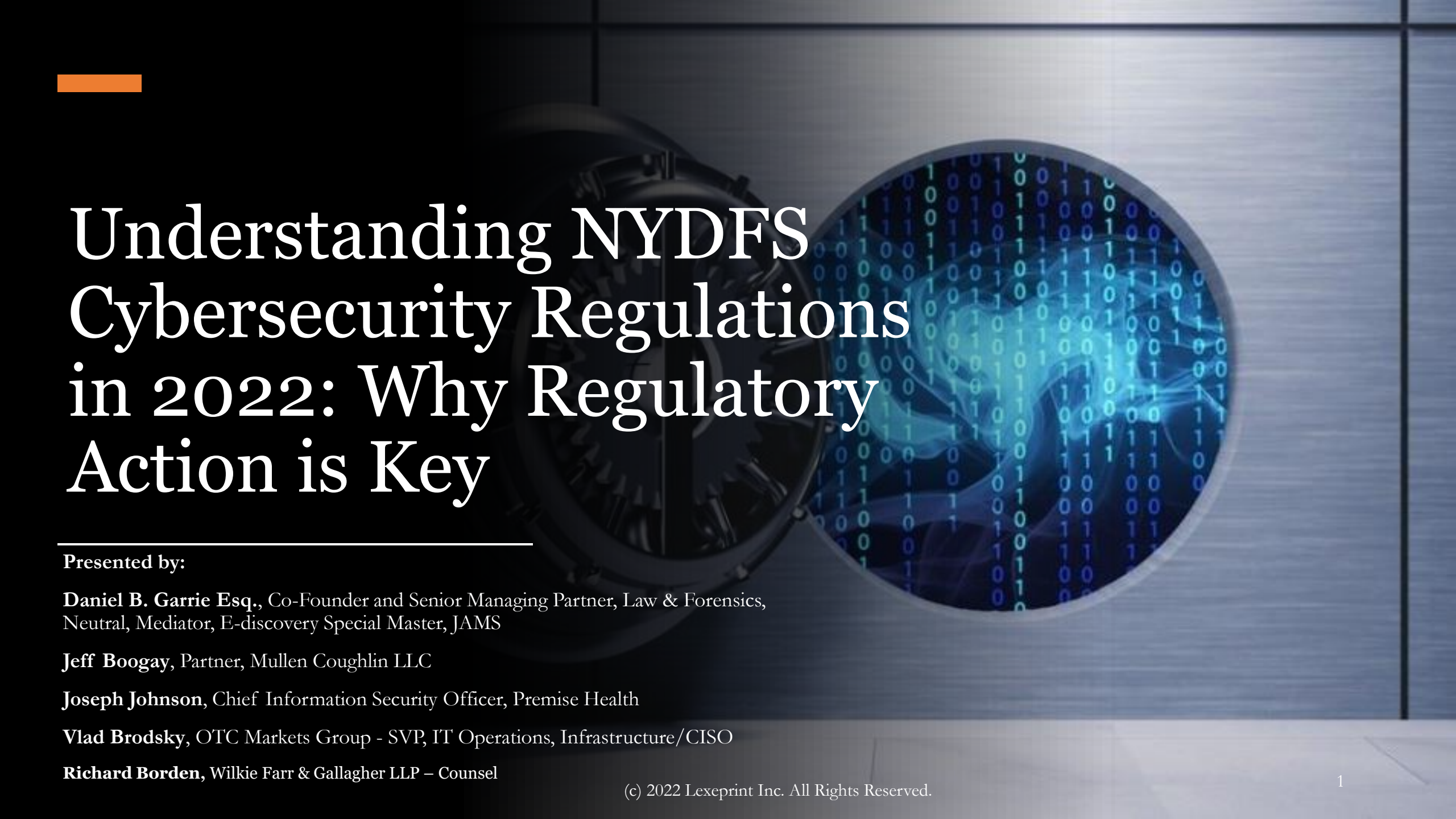
with...

EXPLORE MORE

Overview

Cyber Threat Intelligence Report Volume 2

Cyber Threat Intelligence Report Volume 1



Understanding NYDFS Cybersecurity Regulations in 2022: Why Regulatory Action is Key

Presented by:

Daniel B. Garrie Esq., Co-Founder and Senior Managing Partner, Law & Forensics, Neutral, Mediator, E-discovery Special Master, JAMS

Jeff Boogay, Partner, Mullen Coughlin LLC

Joseph Johnson, Chief Information Security Officer, Premise Health

Vlad Brodsky, OTC Markets Group - SVP, IT Operations, Infrastructure/CISO

Richard Borden, Wilkie Farr & Gallagher LLP – Counsel

(c) 2022 Lexeprint Inc. All Rights Reserved.

Speakers



Daniel B. Garrie, Esq.
Co-founder, Law & Forensics
Mediator, Arbitrator, and
eDiscovery Special Master, JAMS



Jeff Boogay
Partner
Mullen Coughlin LLC



Joey Johnson
Chief Information Security Officer
Premise Health



Vlad Brodsky
OTC Markets Group - SVP, IT
Operations, Infrastructure/CISO



Richard Borden
Wilkie Farr & Gallagher LLP –
Counsel

(c) 2022 Lexeprint Inc. All Rights Reserved.

Disclaimer



This is not legal advice, nor should it be considered legal advice.

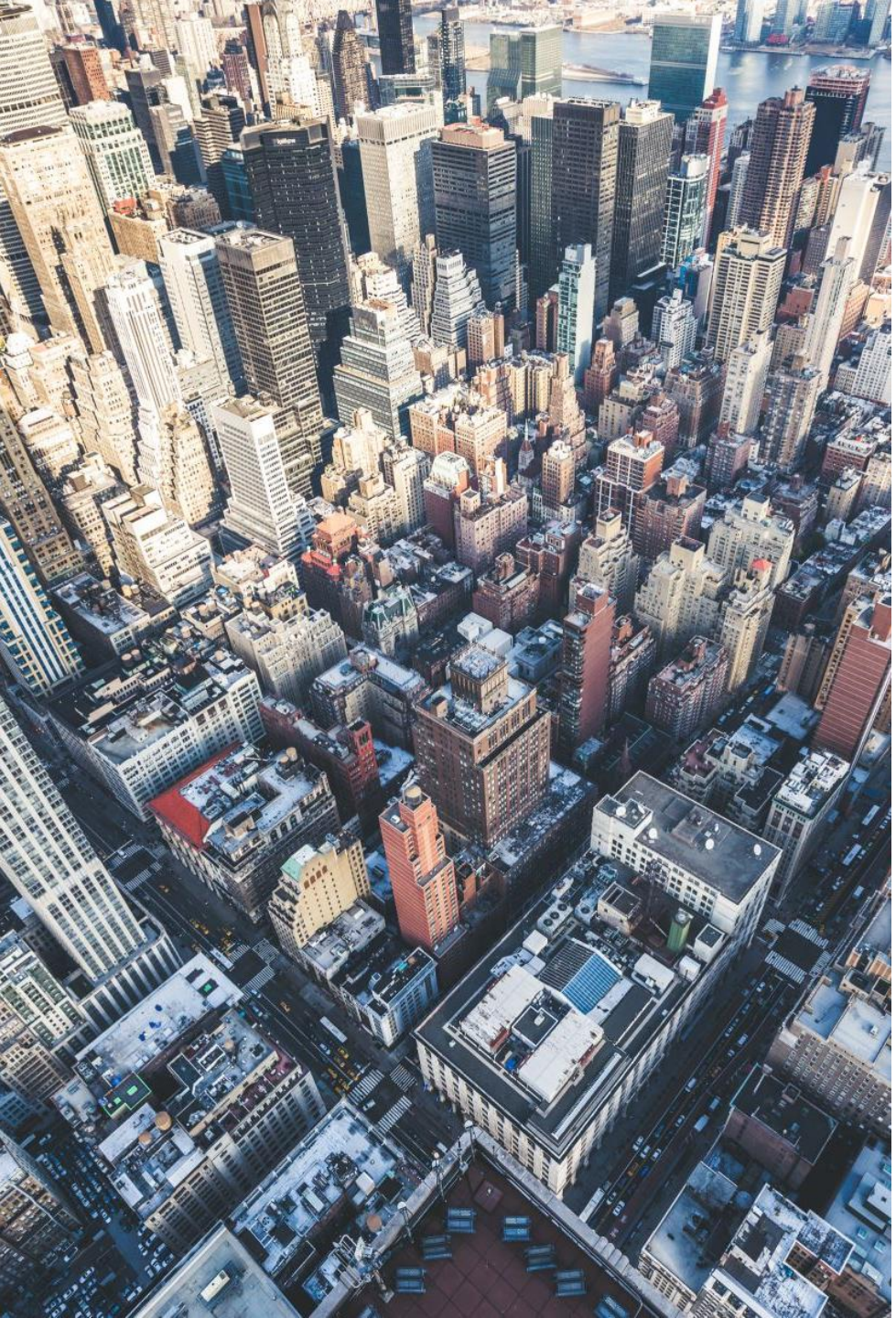


This presentation and the comments contained therein represent only the personal views of the participants, and do not reflect those of their employers or clients.



This presentation is offered for educational and informational uses only.

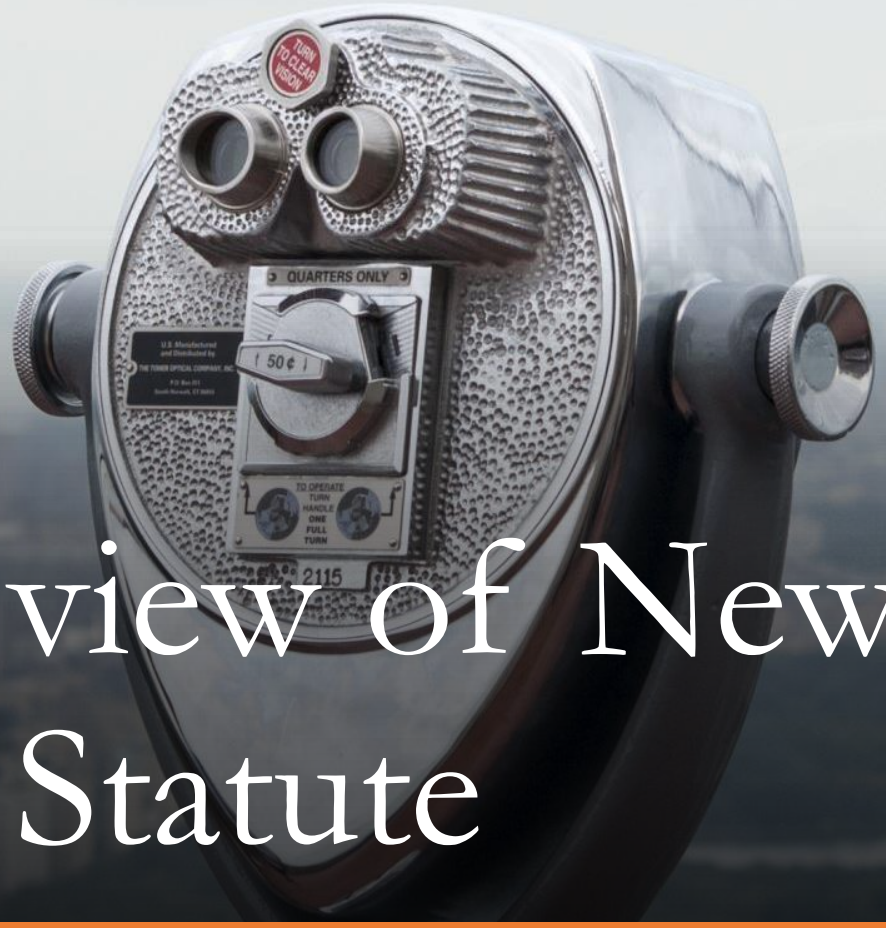
(c) 2022 Lexeprint Inc. All Rights Reserved.



Agenda

- Overview of New York DFS Statute
- Understanding the DFS Statute
- Risk Assessment
- Incident Response Plan

(c) 2022 Lexeprint Inc. All Rights Reserved.



Overview of New York DFS Statute

(c) 2022 Lexeprint Inc. All Rights Reserved.

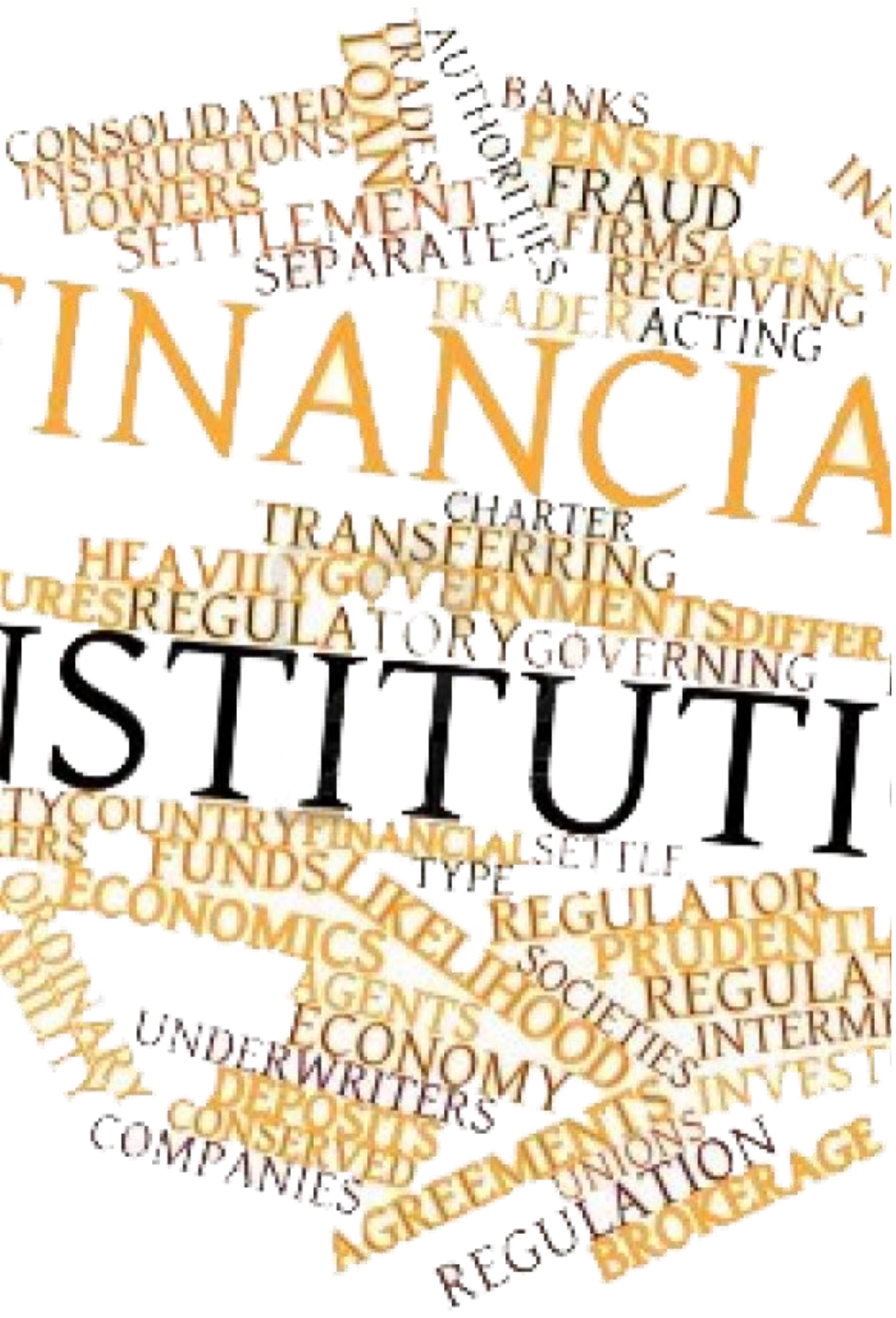


This Photo by Unknown Author is licensed under CC BY

NYDFS Cybersecurity Regulation

- The NYDFS Cybersecurity Regulation enforces cybersecurity guidelines on all covered financial institutions/entities through a four-step implementation process.
- The rules were released on February 16, 2017 and included 23 sections of guidelines to develop and effective cybersecurity measures.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Covered Cybersecurity Regulations

- Covered financial institutions that must follow the regulations include:
  - State-chartered banks
  - Licensed lenders
  - Private bankers
  - Foreign banks licensed to operate in New York
  - Mortgage and insurance companies
  - Service providers

(c) 2022 Lexeprint Inc. All Rights Reserved.



Covered Entities

- Covered Entities are defined as:
  - "[A]ny Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law."
- Exemptions:
  - Small covered entities are exempt from some requirements, including designating a CISO and performing vulnerability assessments each year. - 23 NYCRR 500.01(c)

(c) 2022 Lexeprint Inc. All Rights Reserved.



Why does the NYDFS Regulation matter?

- Studies show that the value at risk globally from cybercrime is estimated at $5.2 trillion dollars from 2019 to 2023.
- The bill is the "first-in-the-nation" regulation concerning cybersecurity and goes beyond other cybersecurity regulations, including the Graham Leach Bliley Act.
- The regulation covers information and systems that do not include, store, process or maintain PII.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Why does the NYDFS Regulation matter?

- The regulation requires new compliance processes and is built around the Risk Assessment to ensure personal data is protected.
- The regulation has forced many covered entities to modify and expand existing protocols to meet regulatory requirements.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Understanding the DFS Statute

(c) 2022 Lexeprint Inc. All Rights Reserved.



Overview of the DFS Regulation – 23 NYCRR 500

- A regulatory system of minimum standards is necessary to promote the protection of customer information and information technology systems.
- The plan includes the following requirements:
  - Cybersecurity program
  - Cybersecurity policy
  - Chief Information Security Officer (CISO)

(c) 2022 Lexeprint Inc. All Rights Reserved.

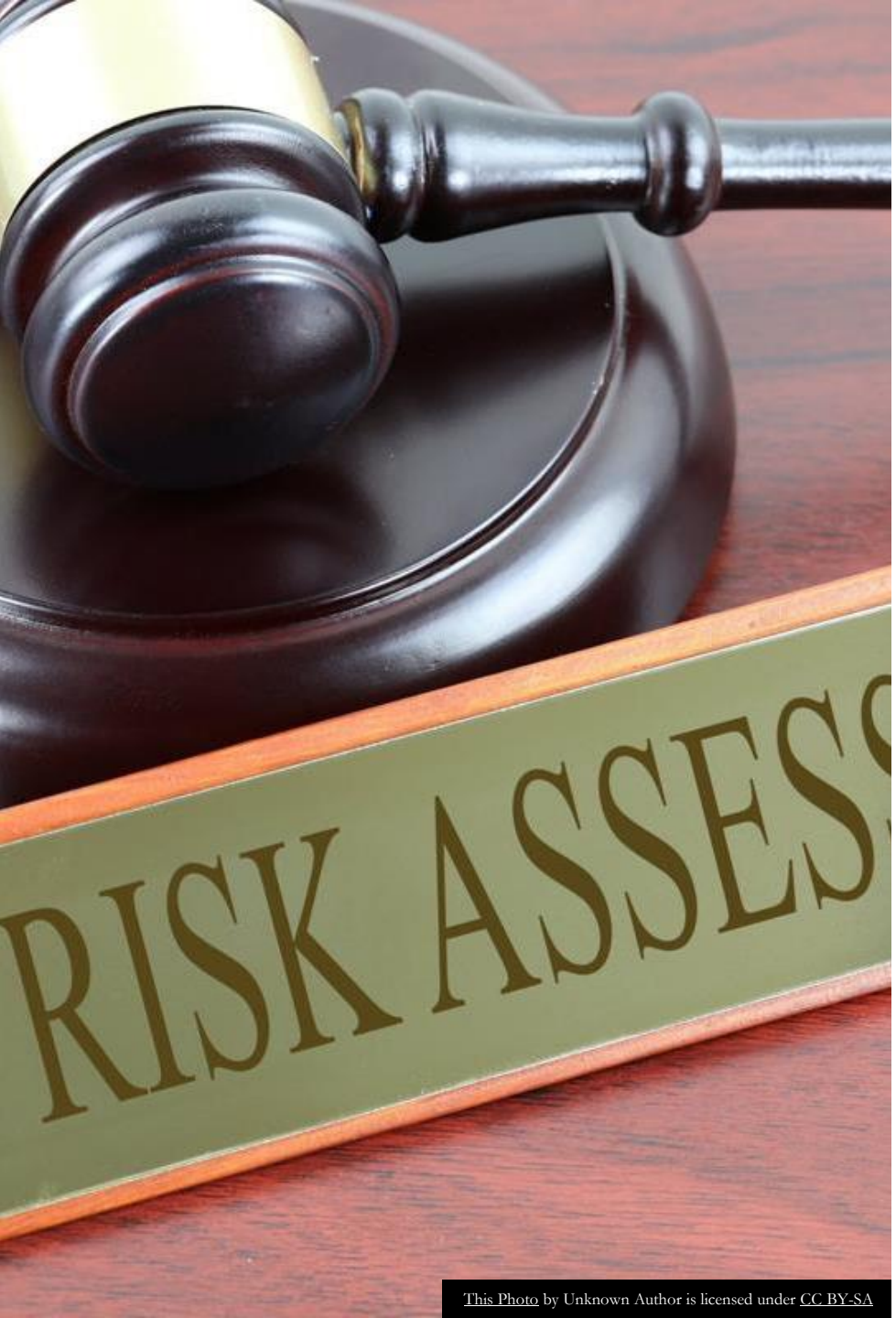


This Photo by Unknown Author is licensed under CC BY-SA

Required Policies and Procedures by DFS Statute

- Risk Assessment (Basis for other policies and procedures/actions)
- Written Cybersecurity Policy
- 3rd Party Information Security Policy
- Limitations on Data Retention
- Training & Monitoring
- Incident & Response Plan
- Application Security

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA

Risk Assessment Requirement 23 NYCRR 500.09(b)

- Risk Assessment is the backbone of the cybersecurity program.
  - Policies and procedures shall include:
    - (1) criteria for the evaluation and categorization of identified risks/threats facing the Covered Entity;
    - (2) criteria for the assessment of the confidentiality, integrity, security & availability of the Covered Entity's Information Systems; and
    - (3) requirements describing how identified risks will be mitigated based on the Risk Assessment and how the cybersecurity program will address them.

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY

Cybersecurity Program 23 NYCRR 500.02

- Each company "shall establish and maintain a cybersecurity program designed to ensure the confidentiality, integrity and availability of the Covered Entity's Information Systems."
- The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform core cybersecurity functions.

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY

Cybersecurity Program 23 NYCRR 500.02

- The written cybersecurity policy mandated by the Regulation must be approved by a "Senior Officer" and requires inclusion of 14 key areas.
- Senior Officers are responsible for the management, operations, security, information systems, compliance and/or risk of a Covered Entity.
- The policy must ultimately be based on the Risk Assessment.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Required Actions

(c) 2022 Lexeprint Inc. All Rights Reserved.



Required Actions By DFS Statute

- Establishment of Qualified Chief Information Security Officer ("CISO")
- Testing Vulnerability Assessments Encryption of Data at Rest and in Transit
- Preservation of Audit Data (to reconstruct transactions and cyber events)
- Data Minimization
- Notices to Superintendent

(c) 2022 Lexeprint Inc. All Rights Reserved.



Chief Information Security Officer (CISO) 23 NYCRR 500.04

- Covered Entities will have to designate a "qualified individual" to serve as the CISO who will be "responsible for overseeing and implementing the [company's] cybersecurity program and enforcing its cybersecurity policy."
- Covered Entities must have cybersecurity personnel sufficient to manage the cybersecurity risks and perform the core functions.
- The CISO will be responsible for producing reports at least annually.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Incident Response Plan

(c) 2022 Lexeprint Inc. All Rights Reserved.



Incident Response Plan and Notice 23 NYCRR 500.16, 500.17

- As part of the cybersecurity program, the Covered Entity must establish an incidence response plan to recover from a cybersecurity breach/attempted breach.
- The entity must provide a notice to the Superintendent within **72** hours from a determination that a cyber incident has occurred and has "a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity."

(c) 2022 Lexeprint Inc. All Rights Reserved.



Incident Response Plan and Notice 23 NYCRR 500.16, 500.17

- The response plan should include:
  - "The internal processes for responding to a cybersecurity event;
  - The goals of the incident response plan;
  - The definition of clear roles, responsibilities and levels of decision-making authority;
  - External and internal communications and information sharing…

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA

Incident Response Plan and Notice 23 NYCRR 500.16, 500.17

- It should also include:
  - Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
  - Documentation and reporting regarding cybersecurity events and related incident response activities; and
  - The evaluation and revision as necessary of the incident response plan following a cybersecurity event."

(c) 2022 Lexeprint Inc. All Rights Reserved.



Questions?

(c) 2022 Lexeprint Inc. All Rights Reserved.

Contact Us



Daniel Garrie
Email: daniel@lawandforensics.com
URL: www.lawandforensics.com



Jeff Boogay
Email: jboogay@mullen.law
URL: https://www.mullen.law/



Richard Borden
Email: rborden@willkie.com
URL: https://www.willkie.com



Joseph Johnson
Email: Joey.johnson@premisehealth.com



Vlad Brodsky
E: vlad@otcmarkets.com
URL: https://www.otcmarkets.com/

(c) 2022 Lexeprint Inc. All Rights Reserved.



Daniel B. Garrie, Esq.
Law & Forensics LLC – Co-Founder
JAMS – Special Master, Neutral, Arbitrator
Contact:
W: (855) 529-2466
E: daniel@lawandforensics.com
URL: https://www.lawandforensics.com/

LAW & FORENSICS
A Global Legal Engineering Firm

B.A., Computer Science, Brandeis Uni.
M.A., Computer Science Brandies Uni.
J.D., Rutgers School of Law

Daniel Garrie, Esq. is the Co-Founder of Law & Forensics LLC, where he heads the Computer Forensics and digital discovery Cybersecurity teams. Daniel has been a dominant voice in the computer forensic and cybersecurity space for the past 20 years, as an attorney and technologist. He is an adjunct professor at Harvard for Computer Forensics and prior to Law & Forensics, he successfully built and sold several technology start-up companies.

Since co-founding Law & Forensics LLC in 2008, Daniel has built it into one of the leading boutique cybersecurity forensic engineering firms in the industry. He is a mediator, arbitrator, and e-discovery special master for JAMS and is a partner and head of the Cybersecurity at Zeichner, Ellman & Krause LLP. Daniel has both a Bachelor's and a Master's degree in computer science from Brandeis University, as well as a J.D. from Rutgers Law School.

Daniel has led cyber and forensic teams in some of the most visible and sensitive cyber incidents in the United States. He and his team have worked for two of the top five banks in the globe, and dozens of the largest private and public companies in the world. In addition, Daniel has been awarded several patents for advanced cybersecurity and forensic platform he built with his team that is currently used in the industry, TableTop.AI, CustodyTrack.IO, and Forensic Scan.

Daniel is also well-published in the cybersecurity space and has authored more than 200 articles and books. His work is cited by Black's Law Dictionary 10th Ed. In defining the terms "software", "internet", and "algorithm." Lastly, he has been recognized by several United States Supreme Court Justices for his legal scholarship and is a trusted source and thought leader for cybersecurity articles and opinions, being cited over 500 times to date.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Jeff Boogay
Mullen Coughlin LLC - Partner
Contact:
E: jboogay@mullen.law
W: (267) 930-4784
URL: https://www.mullen.law/

Jeff Boogay is a Partner at Mullen Coughlin LLC. Mr. Boogay assists clients in both preparation for and response to data security events and regulatory investigations and inquiries.

After a data security event has occurred, Mr. Boogay assists clients in addressing crucial points of fact and law, including: determining the nature and scope of the intrusion; identifying the affected individuals and types of information involved; determining what state, federal and foreign laws govern the client's notice of the incident; and preparing legally compliant notices to affected individuals and appropriate regulators, where required.

Prior to employment with Mullen Coughlin, Mr. Boogay worked for a large international firm where he litigated complex civil cases including allegations of violations of state unfair trade practice statutes.

Mr. Boogay is also a former Assistant District Attorney who worked closely with law enforcement and crime victims to investigate, prepare and litigate criminal cases, and draws on this experience to assist clients.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Joseph Johnson
Premise Health - Chief Information Security Officer
Contact:
E: Joey.johnson@premisehealth.com
URL: www.linkedin.com/in/joey-johnson-6453999/

Premise Health™
Keep your edge.

Joey Johnson is Chief Information Security Officer at Premise Health, provider of large employer sponsor health and wellness centers for employees. Joey is responsible for leading all organizational efforts related to security operations and engineering, information technology and security compliance, identity access management, policy development, security audit, and vendor risk management to meet challenging security and compliance demands. In his six years with Premise Health, Joey has been instrumental in implementing a proactive security and risk management environment focused organizational risk awareness that is transformative in the healthcare industry. He successfully launched a cutting-edge vendor and business associate maturity development program that dynamically empowered business partners of various scales and complexity to meet challenging security and compliance demands. Additionally, he has worked to develop a team driven by passion in security, with a focus on empowering and fostering women in the security field. In 2016 Joey was presented CISO of the Year award by the Nashville Technology Council.

Prior to joining Premise Health, Joey was the Chief Security Officer for the United States Department of Commerce, Office of Computer Services. He has over 15 years of experience in the cyber-security industry including leadership roles in both the public and private sectors, with a focus on organizations in the federal government, information technology, healthcare, and transportation industries. Outside of Premise Health Joey maintains an active leadership presence in the healthcare cyber-security industry participating in numerous steering and advisory committees with the National Healthcare Information Sharing & Analysis Center (NH-ISAC), various threat intelligence and sharing groups, security news groups, and private/public sector partnerships. He serves on the Editorial Board for the Journal of Law and Cyberwarfare helping to shape the future national and international regulatory landscape around cybersecurity, and also works as a senior advisory member on the E-Health Initiative Federal Executive Advisory Board on Privacy & Security. Joey additionally works as a technical advisor with various security & technology investment organizations and product companies, as well as frequently serving as a speaker at numerous security industry events.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Vlad Brodsky
OTC Markets Group - SVP, IT Operations, Infrastructure/CISO
Contact:
W: (212) 896-4464
E: vlad@otcmarkets.com
URL: https://www.otcmarkets.com/

Vlad Brodsky is currently the SVP of IT Operations and Infrastructure and Chief Information Security Officer at OTC Markets Group, a regulated publicly traded financial institution that operates the world's largest electronic marketplace for OTC-traded equities. Vlad's responsibilities include leading the firm's information security strategy, program, and processes. In his four years with OTC Markets Group, Vlad has been instrumental in creating a risk-based information security program that is designed to satisfy business and regulatory requirements.

Vlad has extensive expertise in IT Infrastructure Management, Information Security, and Risk Management. Prior to OTC Markets Group, Vlad worked as a Chief Security Officer for Innovest Systems, a SaaS provider in the Trust Accounting and Wealth Management space, where he was responsible for all Information Security.
Vlad has a Bachelor's degree in Computer Science from Brandeis University, an MBA in Finance and Management from NYU Leonard N. Stern School of Business and holds the CISSP, CRISC, PMP, and FINRA Series 99 certifications. He is also member of the board at New York Metro Infragard – a proactive collaboration between the FBI and the private sector to protect our nation's Critical Infrastructure.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Richard Borden
Wilkie Farr & Gallagher LLP – Counsel
Contact:
Email: rborden@willkie.com
Phone: (212) 728-3872
URL: https://www.willkie.com

WILLKIE
WILLKIE FARR & GALLAGHER LLP

Richard M. Borden is counsel in the Corporate & Financial Services Department and Cybersecurity and Privacy practice group where he focuses on intersecting areas such as technology transactions, cybersecurity and privacy risk management, Fintech and Insurtech.

Rick is at the forefront of cybersecurity and privacy issues, advising on big data governance and the Internet of Things, cybersecurity risk management, and technology sourcing and transactions. Rick translates the often complicated language of technology, cybersecurity, privacy, risk and compliance to assure that it's understood from both a legal and business perspective. His experience on both the customer and vendor side of matters enables him to advise general counsel, C-Suite executives and boards of directors on how to understand potential risks and how to respond should they suffer an incident. Mr .Borden also interfaces with technology departments, advising them on how technology tools and programs may expose companies to risk.

Rick regularly advises clients on data compliance programs, audits and responses to government compliance reviews, privacy policies, data sharing and the collection and use of employee and consumer personal data. He also works with clients to develop bring your own device (BYOD) and mobile computing policies and provides privacy and data protection legal analysis and compliance counseling.

Rick's significant experience across IT and legal sectors enables him to identify risk in light of process, policy and technology, and to effectively communicate with his clients, aligning strategy with their risk management tolerances. He also advises clients on cyber and privacy policies, best practices, reporting, auditing and review, and has extensive experience in regulatory investigations and compliance counseling, data breach insurance policies and claims, corporate risk and reporting, and post-breach penalties and audits.

DATA PROTECTION 101 (/BLOG/SEARCH/DATA-PROTECTION-101)

What is the NYDFS Cybersecurity Regulation? A Cybersecurity Compliance Requirement for Financial Institutions

by Juliana De Groot(https://digitalguardian.com/author/juliana-de-groot) on Tuesday December 1, 2020

arn about the new NYDFS Cybersecurity Regulation and implications for financial institutions in Data Protection , our series on the fundamentals of information security.

EFINITION OF THE NYDFS CYBERSECURITY EGULATION

The NYDFS Cybersecurity Regulation (23 NYCRR 500) (https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf) is a new set of regulations from the NY Department of Financial Services (NYDFS) (http://www.dfs.ny.gov/) that places cybersecurity requirements on all covered financial institutions. The rules were released on February 16th, after two rounds of feedback from the industry and the public and includes sections outlining the requirements for developing and implementing effective cybersecurity program, requiring covered institutions to assess t

effective cybersecurity program, requiring covered institutions to assess t
cybersecurity risks and develop plans to proactively address those risks. NYDFS Cybersecurity Regulation included a phased implementation process, with four distinct phases (https://blog.focal-point.com/understanding-the-4-phases-of-the-nydfs-cybersecurity-regulation-23-nycrr-500) allowing organizations time to implement more robust policies and contr

WHO IS COVERED UNDER THE NYDFS CYBERSECURITY REGULATION?

The NYDFS Cybersecurity Regulation applies to all entities operating unde required to operate under DFS licensure, registration, or charter, or which are otherwise DFS-regulated, as well as, by extension, unregulated third-p service providers to regulated entities. Examples of covered entities incl

- State-chartered banks
- censed lenders
- ivate bankers
- oreign banks licensed to operate in New York
- ortgage companies
- nsurance companies
- Service providers

There are limited exemptions to the NYDFS Cybersecurity Regulat Organizations that employ less than 10 people, produced less than $5 millio gross annual revenue from New York operations in each of the past three ye or hold less than $10 million in year-end total assets are exempt from cer requirements of the Regulation.

HOW THE NYDFS CYBERSECURITY REGULATION

HOW THE NYDFS CYBERSECURITY REGULATION WORKS

The NYDFS Cybersecurity Regulation works by imposing strict cybersecu rules on covered organizations, including the installment of a detailed cybersecurity plan, the designation of Chief Information Security Officer (CISO) (https://digitalguardian.com/blog/anatomy-ciso-breakdown-todays-top-security-leaders-infographic), the enactment of a comprehensive cybersecurity policy, and the initiation and maintenance of an ongoing repor system for cybersecurity events. These components are all made up of seve sub-regulations and requirement

NYDFS CYBERSECURITY REGULATION REQUIREMENTS

A cybersecurity program that complies with the new NYDFS Cybersecu Regulation will adhere to several key requirements, aligned to the NIST

- ersecurity Framework (https://digitalguardian.com/blog/what-nist-npliance):
- entify all cybersecurity threats, both internal and external.
- nploy defense infrastructure to protect against those threats.
- Use a system to detect cybersecurity events.
- Respond to all detected cybersecurity events.
- Work to recover from each cybersecurity event.
- Fulfill various requirements for regulatory reporting.

CYBERSECURITY POLICY DESIGN

The initial phase of the NYDFS Cybersecurity Regulation went into effec February 15, 2018 and requires covered organizations to develop a cybersecu

policy, including an incident response plan that includes data breach notifications within 72 hours. The policy must address concerns in alignment with industry best practices ar ISO 27001 standards (http://www.iso27001security.com/html/27001.html). Most notably, the policy must cover:

- Information security
- Access controls
- Disaster recovery planning
- Systems and network security
- Customer data privacy
- Regular risk assessments

PORTING PROCEDURES

se two, which went into effect on March 1, 2018, requires CISOs to prepare annual report that include

- ıe organization's cybersecurity policies and procedures
- ıe organization's security risks
- The effectiveness of the organization's existing cybersecurity measures

Covered institutions are required to develop and implement a cybersecu program that continuously evaluates vulnerabilities, which not only informs the annual report but also enables the organization to develop proactive respor to threats

PROGRAM DEVELOPMENT

Phase three, which went into effect on September 3, 2018, requires covered

institutions to have a comprehensive cybersecurity program in place that contains several key elements, includin

- An audit trail that reflects threat detection and response activities
- Written documentation of procedures, standards, and guidelines for in-house applications as well as procedures for evaluating third-party applications
- Detailed data retention policy documentation, including how non-public personal information is disposed
- Encryption and other robust security control measures

THIRD PARTY SECURITY

The final remaining requirement (https://medium.com/@Soteria_Security/nydfs-cybersecurity-compliance-requirements-589b05027509) was effective as of March 1, 2019. This requirement states that covered institut

- to finalize their policies regarding any third party which could be g
- missions to access systems and files covered by the regulation. Covered
- ncial institutions are required to develop a written policy for third-p
- urity that detail
- sk assessment of third-party service providers
- The covered financial institution's security requirements of third-party service providers that must be met in order to conduct business with that entity
- Processes for evaluating the effectiveness of a third-party service provider's security practices
- Periodic assessments of third-party policies and controls

ADDITIONAL REQUIREMENTS

Organizations covered by the NYDFS Cybersecurity Regulation are also requ

to:

- Use qualified, continuously trained cybersecurity personnel to manage evolving cybersecurity threats and responses. These can be third party actors.
- Notify the NYDFS about all cybersecurity events that carry a "reasonable likelihood" of causing material harm.
- Limit access privileges. Companies covered by the regulation must monitor and limit access privileges granted to users.

COVERED INSTITUTIONS MUST ADDRESS NEW CYBERSECURITY CHALLENGES

Some requirements of the NYDFS Cybersecurity Regulation go above a
beyond existing industry best practices. The most noteworthy are:

- Data encryption: Organizations must enact controls, including encryption of
  ensitive data, depending on the outcome of a risk assessment.
- nnual certification: Covered entities must complete certification every year
  confirm compliance with the regulations.
- nhanced multi-factor authentication: Covered institutions must employ
  ulti-factor authentication (https://www.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf) for all inbound connections to the entity's network.
- Incident reporting: Covered entities must document and report all cybersecurity events.

CONSEQUENCES AND PENALTIES FOR NYDFS CYBERSECURITY REGULATION VIOLATIONS

As the regulation currently sits, there are no details regarding fines

violations. However, penalties will be calculated for violations, leaving amount unknown for covered entities. Once the regulation is fully in force in Spring of 2019, violations may be alleged and founded. The fees and ot ramifications may become public knowledge if such violations occur.

Note: When publicly questioned about the language and fees required of violators, drafters of the NYDFS offered no further explanati

BENEFITS AND DRAWBACKS OF THE NYDFS CYBERSECURITY REGULATION

The NYDFS Cybersecurity Regulation was adopted on March 1, 2017 after a l history of damaging cyber attacks and data breaches in the financial industry. While NYDFS paved the way for other states to enact much-neec cybersecurity regulation, their efforts may not go far enough. In no partic order, here are a few pros and cons surrounding the new regulat

- ıe regulation has been scaled back from proposed versions, which called for
- ıe encryption of all data at rest and in transit, which many institutions gued was unnecessarily restrictive.
- :cording to Sam Olyaei, senior research analyst at Gartner Research, the gulation waswoefully out of date(http://blogs.gartner.com/sam-olyaei /2017/03/01/ny-dfs-cybersecurity-requirements-go-effect-today-already-outdated/) even before its enactment, though he admits it's much better than regulation in place (or not in place) in other states.

Organizations with less than 10 employees and independent contractors are considered exempt under the enacted version of the regulation.

Small and medium-sized companies can rely on third party service providers to meet many of the regulation requirements.

BEST PRACTICES FOR COMPLYING WITH NYDFS

BEST PRACTICES FOR COMPLYING WITH NYDFS CYBERSECURITY REGULATION

Financial institutions face a near-term compliance challenge in the face of new NYDFS Cybersecurity Regulation. Best practices involve meeting all the requirements in a timely manner, paying special attention to deadlines, and appointing a qualified CISO to pull together an appropriate response preparing for NYDFS Cybersecurity Regulation compliance, be sure to:

Assess whether your institution classifies as "covered." There are several exemptions, but exempt organizations must file as such within 30 days of the end of the most recent fiscal year. To determine whether your organization is "covered," see the NYDFS website's "Who We Supervise" page here (http://www.dfs.ny.gov/about/whowesupervise.htm).

Assemble your organization's regulatory compliance team. All covered, non-exempt financial institutions should have assigned a Chief Information Security Officer (CISO). While the CISO holds overarching responsibility for compliance, achieving and maintaining compliance is generally a job for a team rather than an individual, especially considering that the new regulations apply enterprise-wide.

Understand your risk profile. The required Risk Assessment was required to be submitted by March 1, 2018. However, organizations should be conducting ongoing, periodic risk assessments to identify vulnerabilities and respond proactively to emerging threats.

Adhere to all deadlines. The final provisions in the new regulation went into effect on March 1, 2019. See the full regulation document here (http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf) for clarification.

ADDITIONAL RESOURCES ON THE NYDFS

CYBERSECURITY REGULATION

For more information about the NYDFS Cybersecurity Regulation, visit the following resources

- See the NYDFS "Who We Supervise" page (http://www.dfs.ny.gov/about/whowesupervise.htm) to assess whether your institution is covered under NYDFS Cybersecurity Regulation.
- The NYDFS regulation document is viewable in PDF form here (http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf)
- The NYDFS Regulation FAQs page is here (http://www.dfs.ny.gov/about/cybersecurity_faqs.htm). It answers 14 commonly asked questions about the regulation, including questions about deadlines, requirements, and definitions.

Tags: Data Protection 101 (/blog/search/data-protection-101), Compliance (/blog/search/compliance), Financial Services (/blog/search/financial-services), Industry Insights (/blog/search/industry-insights)

PRIMER ON THE NEW NYDFS CYBERSECURITY REGULATION

BY JEEWON KIM SERRATO, COUNSEL AND REENA SAHNI, PARTNER AT SHEARMAN & STERLING LLP.

The New York Department of Financial Services (NYDFS) Cybersecurity Requirements for Financial Services Companies (the Final Regulation)[1] took effect on March 1, 2017. We discussed in our earlier publication the background on how the original proposal of the regulation was updated in the context of other recent developments in the financial services industry.[2] In the introductory section (§ 500.00) of the Final Regulation, the NYDFS stated that: "The financial services industry is a significant target of cybersecurity threats…Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted… Adoption of the program outlined in these regulations is a priority for New York State."

The NYDFS regulation confirms once more how cybersecurity concerns are at the top of the agenda of priorities for many state and federal regulators in the banking and financial services industry. Pursuant to the Final Regulation, certain banks, insurers and other financial services institutions holding a New York state license will be required to conduct periodic assessments of their cybersecurity risks and implement and maintain a cybersecurity program designed to address such risks.

Who is affected?

The regulation applies to any entity that holds a certificate, permit, accreditation or similar authorization under banking, insurance or financial services laws (each, a covered entity). The definition appears to be broad, especially considering that the concept of "similar authorization" may apply to service providers and/or independent contractors of covered entities operating under any relevant certificate or permit required by New York banking, insurance or financial services law.

Affiliates and extraterrestrial research

Comment letters on the Original Proposed Regulation raised concerns with respect to the extraterritorial scope – in particular with respect to the broad definition of foreign banking organizations (FBOs).

In response, the NYDFS clarified that a New York branch of a foreign bank falls within the definition of covered entity, and therefore is subject to the applicable cybersecurity requirements. In addition, the Final Regulation provides that a covered entity can satisfy the applicable cybersecurity requirements by adopting a cybersecurity program maintained by an affiliate (defined in § 500.01) provided that the affiliate's program is compliant with the applicable cybersecurity requirements introduced by the NYDFS. Therefore, under the Final Regulation, the New York branch of an FBO may comply with the newly introduced cybersecurity requirements either by:

- Establishing and maintaining its own cybersecurity program, or
- Adopting the program of the FBO itself, if it is compliant with the regulation.

Exemptions

The Final Regulation includes an exemption from some of the cybersecurity requirements for covered entities whose number of employees, revenues and assets do not exceed certain thresholds. Covered entities meeting any of the following criteria are exempted from a number of cybersecurity requirements under the Final Regulation (including the requirements to appoint a CISO, encrypt non-public information, and adopt an incident response plan):

- Fewer than 10 employees, including any independent contractors of the covered entity or its affiliates located in New York or responsible for business of the covered entity

> "The financial services industry is a significant target of cybersecurity threats …given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted."
>
> The New York Department of Financial Services

1 Available at http: http://www.dfs.ny.gov/legal/regulations/adoptions/rf23-nycrr-500_cybersecurity.pdf (23 N.Y.C.R.R. pt. 500).
2 Available at http://www.shearman.com/en/newsinsights/publications/2017/01/cybersecurity-protection-of-financial-data

- Less than $5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations of the covered entity and its affiliates
- Less than $10,000,000 in year-end total assets, calculated in accordance with GAAP, including assets of all Affiliates

In addition, the limited exemption applicable to covered entities with less than $5 million in gross revenue for each of the last three fiscal years is now further expanded to include covered entities with less than $5 million in gross revenue "from its New York business operations (or its affiliates' operations)." Therefore, certain larger financial institutions with smaller New York operations may now qualify for either of these new exemptions. Each covered entity that qualifies for the exemption above is required to file a Notice of Exemption with the NYDFS.

Timeline for compliance

The regulation went into effect on March 1, 2017. Pursuant to the Final Regulation, each Covered Entity is required to establish and maintain a cybersecurity program tailored to address the certain critical cybersecurity concerns by August 28, 2017 (180 days from the effective date). This program should include the following elements, among others:

- Written cybersecurity policy (§ 500.03)
- Appointment of a chief information security officer (CISO) (§ 500.04(a)) and additional cybersecurity personnel (§ 500.10)
- Access privileges to protect non-public information (§ 500.07) Incident response plan designed to promptly respond to a cybersecurity event (§ 500.16)
- Procedures to promptly notify NYDFS of any cybersecurity events (§ 500.17)

One of the main changes from earlier proposals is that the Final Regulation allows for a more flexible and risk-based approach. Compared to the Original Proposed Regulation, which drew criticism because it was seen as a one-size-fits-all approach, the covered entity's cybersecurity program may now use risk assessments to identify the particular risks that are relevant to its business operations and assess the availability and effectiveness of controls that are designed to respond to those threats. Each covered entity is required to conduct the risk assessment periodically (and not annually as provided for by the Original Proposed Regulation).

The implementation of the program will provide covered entities with the foundation for a robust and successful plan to protect against cyber threats.

CISO report, testing and training

A number of requirements detailed in the Final Regulation have a 12-month transition period for covered entities to comply. These requirements must be met by March 1, 2018:

- CISO report on the covered entity's program (§ 500.04(b))
- Testing and vulnerability assessments (§ 500.05)
- Periodic risk assessments (§ 500.09)
- Multi-factor authentication to protect non-public information (§ 500.12)
- Cybersecurity awareness training for all personnel (§ 500.14(b))

Cybersecurity risks and third-party service providers

Further requirements of the Final Regulation have an 18-month transitional period for compliance and must be implemented by September 1, 2018. These include:

- Audit trail (§ 500.06)
- Application security policies for the development of in-house applications (§ 500.08)
- Data retention policies (§ 500.13)
- Monitoring of authorized users (§ 500.14(a))
- Encryption of nonpublic information (§ 500.15)

Risk management for third-party service providers

The Final Regulation specifically addresses scenarios under which third-party service providers have access or hold non-public information pertaining to a covered entity (§ 500.11). Covered entities will have until March 1, 2019 (two years from the effective date) to implement policies related to third-party service providers.

In those circumstances, a covered entity is required to implement written policies and procedures to ensure the security and integrity of such non-public information, by providing for:

- Minimum cybersecurity practices to be met by third-party service providers
- Due diligence processes to evaluate the adequacy of the cybersecurity practices of third-party service providers
- Periodic assessments of third-party service providers from a cybersecurity risk management perspective

Conclusion

The cybersecurity regulation adopted by the NYDFS imposes significant new requirements and obligations on covered entities. In light of the 180-day compliance window and the staggered implementation schedule, covered entities should immediately begin assessing their cybersecurity risks, implementing effective policies and developing robust cybersecurity programs to achieve compliance with the new cybersecurity requirements.

Part of the Mergermarket Group

www.mergermarketgroup.com

330 Hudson St. FL 4
New York, NY 10013
USA

t: +1 212.686.5606
f: +1 212.686.2664
sales.us@mergermarket.com

10 Queen Street Place
London
EC4R 1BE
United Kingdom

t: +44 (0)20 7059 6100
f: +44 (0)20 7059 6101
sales@mergermarket.com

Suite 1602-6
Grand Millennium Plaza
181 Queen's Road, Central
Hong Kong

t: +852 2158 9700
f: +852 2158 9701
sales.asia@mergermarket.com

Disclaimer
This publication contains general information and is not intended to be comprehensive nor to provide financial, investment, legal, tax or other professional advice or services. This publication is not a substitute for such professional advice or services, and it should not be acted on or relied upon or used as a basis for any investment or other decision or action that may affect you or your business. Before taking any such decision, you should consult a suitably qualified professional advisor. Whilst reasonable effort has been made to ensure the accuracy of the information contained in this publication, this cannot be guaranteed and neither mergermarket nor any of its subsidiaries or any affiliate thereof or other related entity shall have any liability to any person or entity which relies on the information contained in this publication, including incidental or consequential damages arising from errors or omissions. Any such reliance is solely at the user's risk.

LEXOLOGY

NYDFS Publishes Pre-Proposed Amendment to Cybersecurity Regulations ("Part 500")

Schulte Roth & Zabel LLP

USA | August 15 2022

On July 29, 2022, the New York State Department of Financial Services ("NYDFS") published pre-proposal amendments ("Proposed Amendments")[1] to its **cybersecurity regulations** ("Part 500").[2] While **NYDFS** will be accepting comments on the Proposed Amendments through its website until Aug. 18, 2022, there will still be a full 60-day notice and comment period before the amendments are final.

Key provisions of NYDFS's Proposed Amendments include: (1) new notification requirements; (2) new obligations for "Class A" companies; (3) new requirements concerning entity governance; (4) modifications to the compliance certification requirement; and (5) clarifications around penalties.

1. Notification Requirements

The Proposed Amendments would add additional reporting requirements, including the requirement to notify the **NYDFS** within 72 hours of any unauthorized access to privileged accounts or deployment of ransomware within a material part of an entity's information systems. It should be noted that this requirement is in addition to the already existing requirement to notify **NYDFS** within 72 hours of any **cybersecurity** events that require notice to any supervisory body or that have a reasonable likelihood of materially harming a material part of an entity's normal operations. Furthermore, the Proposed Amendments would add a new 24-hour notification obligation for ransomware payments, and a corresponding 30-day reporting requirement within which an entity must provide a written explanation of why payment was necessary, alternatives to payment that were considered and sanctions diligence that was conducted.

2. Obligations for Class A Companies

The Proposed Amendments would impose requirements on a new category of covered entities, "Class A" companies, which are defined as covered entities with either (1) over 2,000 employees or (2) over $1 billion in gross annual revenue averaged over the previous three years from all business operations of the covered entity and its affiliates. Under the Proposed Amendments, Class A companies must: (1) conduct independent audits of the **cybersecurity** program, at least annually; (2) conduct vulnerability assessments (such as systematic scans or reviews) at least weekly; (3) implement mandatory password vaulting solutions for privileged accounts; (4) maintain an endpoint detection and response solution to monitor anomalous activity, as well as a solution for centralized logging and security event alerting; and (5) utilize external experts to conduct a risk assessment at least once every three years.

3. Enhanced Governance Requirements

The Proposed Amendments would add additional requirements concerning entity governance. More specifically, the Proposed Amendments would require that, among other additional obligations: (1) the Chief Information Security

Officer ("CISO") have adequate independence and authority to ensure appropriate management of **cybersecurity** risks; (2) the CISO provide the board with additional detailed annual reporting on plans for remediating inadequacies, as well as timely reports regarding material **cybersecurity** issues or events; (3) the entity's **cybersecurity** policy be approved by the board, rather than senior management; and (4) an entity's board have sufficient knowledge and expertise (or be advised by persons with sufficient knowledge and expertise) to exercise effective oversight of **cybersecurity** risk.

4. Certification/Acknowledgment of Compliance Modifications

The Proposed Amendments would require that the annual certification of compliance be signed by the CEO and the CISO (or the CEO and senior officer responsible for the **cybersecurity** program where the entity lacks a CISO). The Proposed Amendments would also allow entities to submit an acknowledgment of less-than-full compliance for the prior calendar year. An entity which submits an acknowledgment of less-than-full compliance must also identify the **cybersecurity** program's specific deficiencies, describe the nature and extent of noncompliance and identify the systems, areas and processes which require material improvement, updating or redesign. Furthermore, an entity which submits an acknowledgment of less-than-full compliance must be ready to provide **NYDFS** with documentation detailing the remedial efforts planned and underway, along with a timeline for implementing those efforts.

5. Penalty Clarifications

The Proposed Amendments would provide additional clarity concerning NYDFS's penalty calculation process. For example, the Proposed Amendments note that the commission of a single act prohibited by Part 500, or the failure to satisfy an obligation required by Part 500, constitutes a violation, including an entity's failure to comply for any 24-hour period with any section or subsection of Part 500. In addition, the Proposed Amendments include a list of factors that **NYDFS** will consider when assessing a penalty (e.g., cooperation, good faith, isolated incident v. systemic violations, etc.).

Moving Forward

While this *Alert* is not an exhaustive list of the modifications contained in the Proposed Amendments, it is intended to highlight key provisions of the Proposed Amendments, should these proposed provisions be finalized and adopted.

Schulte Roth & Zabel LLP - Donald J. Mosher, Kara A. Kuchar , Melissa G.R. Goldstein, Adam J. Barazani, Jessica Romano, Jessica Sklute, Noah N. Gillespie, Rebecca A. Raskind and Jesse Weissman

Powered by
LEXOLOGY.

NYDFS propose new cybersecurity regulations, effective Jan 1 2017. Here's what you need to know

Posted by: Carole Theriault



2
NOV
0

Last month, the New York State Department of Financial Services (NYDFS) put forward a proposed regulation designed to impose new rigorous cybersecurity requirements on banks, consumer lenders, money transmitters, insurance companies as well as some financial service providers in New York State.

The State has indicated that securing both New York's financial services firms and its consumers is the main priority. The aim is to lower the risk posture in light of the threats posed by "nation-states, terrorist organizations, and independent criminal actors."

So far, so good. But affected firms need to get their skates on pronto. The effective date is January 1, just two months from now.

The impact is of course much broader than just New York State. Even "Non-U.S. insurers and reinsurers in particular will want to confirm if the proposed regulation applies – whether with respect to excess lines insurers, "trusteed" or "certified" reinsurers," writes US law-firm Drinker Biddle.

Summary of the NYDFS cybersecurity proposal

Make no mistake – the requirements outlined below are of Clydesdale proportions. Experts at TBG security strongly recommend a comprehensive internal review to ensure everything is in place before the new year gallops into the present.

So what's involved? Here is the high-level list:

Cybersecurity Program. Each Covered Entity shall establish and maintain a cybersecurity program designed to ensure the confidentiality, integrity and availability of the Covered Entity's Information Systems.

Cybersecurity Policy. Each Covered Entity shall implement and maintain a written cybersecurity policy setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information *(see Note 1 below)* stored on those Information Systems.

Chief Information Security Officer. Each Covered Entity shall designate a qualified individual to serve as the Covered Entity's Chief Information Security Officer ("CISO") responsible for overseeing and implementing the Covered

TBG Cybersecurity News

Sign up for Cybersecurity News

Please enter your email

Subscribe

Recent Posts

- Kaseya and REvil: two sides of the supply-chain risk story
- IoT device makers wanting to better security standards
- Hafnium and SolarWinds shake up attitudes to supply chain risk management
- Takeaways from the British Mensa Security Drama
- Remember Online Scams Target Businesses Too

Posts By Category

Select Category
201 CMR 17.00 (9)

Blog Archive

Select Month

Data Breach News

Support

Entity's cybersecurity program and enforcing its cybersecurity policy.

Penetration Testing and Vulnerability Assessments. The cybersecurity program for each Covered Entity shall, at a minimum, include penetration testing of the Covered Entity's Information Systems at least annually and vulnerability assessment of the Covered Entity's Information Systems at least quarterly.

Audit Trail. The cybersecurity program for each Covered Entity shall, at a minimum, include implementing and maintaining audit trail systems.

Access Privileges. Each Covered Entity shall limit access privileges to Information Systems that provide access to Nonpublic Information solely to those individuals who require such access to such systems in order to perform their responsibilities and shall periodically review such access privileges.

Risk Assessment. At least annually, each Covered Entity shall conduct a risk assessment of the Information Systems. Such risk assessment shall be carried out in accordance with written policies and procedures and shall be documented in writing.

Cybersecurity Personnel and Intelligence. each Covered Entity shall employ (or use a qualified third party) to perform the duties of cybersecurity personnel, including managing the Covered Entity's cybersecurity risks and performing the core cybersecurity functions.

Third Party Information Security Policy. Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, third parties doing business with the Covered Entity.

Multi-Factor Authentication. Each Covered Entity shall require Multi-Factor Authentication for any individual in order to access the internal systems or data from an external network; to access web applications that capture, display or interface with Nonpublic Information, and to support Multi-Factor Authentication for any individual accessing web applications that capture, display or interface with Nonpublic Information.

Limitations on Data Retention. Each Covered Entity shall include policies and procedures for the timely destruction of any Nonpublic Information identified no longer necessary for the provision of the products or services.

Training and Monitoring. Each Covered Entity shall implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users as well as require all personnel to attend regular cybersecurity awareness training sessions

Encryption of Nonpublic Information. Each Covered Entity shall encrypt all Nonpublic Information held or transmitted by the Covered Entity both in transit and at rest, where feasible.

Incident Response Plan. Each Covered Entity shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business.

Notices to Superintendent. Each Covered Entity shall notify the superintendent of any Cybersecurity Event that has a reasonable likelihood of materially affecting the normal operation of the Covered Entity or that affects Nonpublic Information. The Covered Entity must notify the superintendent as promptly as possible but in no event later than 72 hours after becoming aware of such a Cybersecurity Event.

Read New York state's proposal yourself: CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES [PDF]

"In order to meet the Jan. 1, 2017 effective date, Covered Entities should now begin assessing their cybersecurity risks, policies and procedures to develop

TBG Cybersecurity News
Recent Posts
Kaseya and REvil: two sides of the supply-chain risk story
IoT device makers wanting to better security standards
Hafnium and SolarWinds
Shake up attitudes to supply chain risk management
Takeaways from the British Mensa Security Drama
Remember Online Scams Target Businesses Too
Posts By Category
Select Category
201 CMR 17.00 (9)
Blog Archive
Select Month
Data Breach News

or enhance their cybersecurity program and to begin documenting and tracking their compliance efforts," says the Harvard Law School Forum on Corporate Governance and Financial Regulation.

We couldn't agree more. And get in touch with us if you need clarification, advice, strategic counsel and/or cybersecurity expertise. We're here to help.

NOTE 1: The term 'Nonpublic information' encompasses far more than the previously defined term 'Personal Information.' According to Schiltz, Roth and Zable "Most notably, the Proposed Regulation has several directives tied to 'Nonpublic Information,' and it defines that term broadly, including any information that would be considered nonpublic personal information under the Gramm-Leach-Bliley Act's privacy rule ("GLBA Privacy Rule"). As a result, it captures far more data than what New York's existing data protection law defines as "personal information."[2] The requirement that "Nonpublic Information" be encrypted at rest (and not just in transit) may therefore be a significant burden on Covered Entities, as may the requirement that the Superintendent be notified of any 'Cybersecurity Event' that "affects" Nonpublic Information. Further, senior management must certify annually that the Covered Entity is in compliance."

About TBG Security Inc.

TBG Security is a leading provider of information security and risk management consulting for Fortune 100 and Fortune 500 companies. TBG designs and delivers cyber security solutions to work in harmony with existing operations. Companies depend on TBG services in areas including risk [illegible]ecurity policy development, security strategies for compliance, business continuity, network security, managed services, software and service integration and incident response.

For more information on how TBG Security can help your organization with your information security initiatives please visit https://tbgsecurity.com.

RELATED POSTS

- How the pandemic changed everything and nothing
- Backup Strategy in six points (and a free mnemonic)
- Why it is high time to consider a CISO on demand
- Isn't it time we talk seriously about a nation-wide Privacy Act?
- Should C-level Bonuses Be Tied To Cybersecurity Posture?

TBG Cybersecurity News

Recent Posts
- Kaseya and REvil: two sides of the supply-chain risk story
- IoT device makers wanting to better security standards
- Hafnium and SolarWinds shake up attitudes to supply chain risk management
- Takeaways from the British Mensa Security Drama
- Remember Online Scams Target Businesses Too

Posts By Category
Select Category
201 CMR 17.00 (9)

Blog Archive
Select Month

Data Breach News

TBG Security Inc.
31 Hayward St.
Franklin, MA 02038
P (877)-233-6651
F (508)-355-5782
Email: info@tbgsecurity.com

t of secure

TBG Cybersecurity News

© TBG Security 2003-2020 | Privacy Statement | Do Not Sell My Personal Information



Recent Posts

- Kaseya and REvil: two sides of the supply-chain risk story
- IoT device makers wanting to better security standards
- Hafnium and SolarWinds shake up attitudes to supply chain risk management
- Takeaways from the British Mensa Security Drama
- Remember Online Scams Target Businesses Too

Posts By Category

Select Category

201 CMR 17.00 (9)

Blog Archive

Select Month

Data Breach News

February 27, 2017

Ari Schwartz

New York's Department of Financial Services Finalizes Cybersecurity Requirements for Financial Institutions

3min

On March 1, 2017, the New York State Department of Financial Services' (DFS) mandatory cybersecurity requirements for financial services entities will become effective, with implementation to occur within 180 days (or by September 1, 2017). The requirements broadly cover all entities operating under or required to operate under DFS licensure, registration, or charter, or which are otherwise DFS-regulated, as well as, by extension, unregulated third-party service providers to regulated entities. This not only includes state-chartered banks, licensed lenders, private bankers, service contract providers, trust companies, and mortgage companies, but also foreign banks licensed to operate in New York and any insurance company doing business in New York. It does exempt small companies, though, including those with fewer than 10 employees, less than $5 million in gross annual revenue for three years, or less than $10 million in year-end total assets.

The regulation delineates various minimum standards and requires a risk-based cybersecurity program tailored to each company's specific risk profile. Significantly, the regulation requires covered entities to file an annual certification of compliance with the regulation; Certifications of Compliance will commence February 15, 2018.

As discussed in a prior alert, DFS proposed similar regulations on September 13 of last year, but that set of regulations elicited significant feedback. Still, the regulations require potentially significant changes and focus on cybersecurity for many institutions.

Requirements

Generally, the regulation's requirements are focused on steps to increase security awareness and to encourage a risk-based, holistic, and robust security program at covered entities. To ensure compliance, covered entities must implement the following:

1. *Risk Assessments:* Periodic risk assessments that consider threats, particular risks to the entity, and an examination of existing controls in the context of identified risk.
2. *Cybersecurity Program:* The creation of a cybersecurity program based on the periodic risk assessments and designed to identify and assess risks; protect information systems and nonpublic information; detect, respond to, and recover from cyber events; and fulfill all reporting obligations. The program must include annual penetration testing and biannual vulnerability assessments. The cybersecurity program referenced here follows the general mandates of those

delineated in the NIST Cybersecurity Framework.

3. *Cybersecurity Policies*: The creation and maintenance of written policies and procedures for the protection of information systems and nonpublic information and based on the risk assessment. These must include a written incident response plan.
4. CISO: The designation of a chief information security officer to oversee the cybersecurity program.
5. *Minimum Standards*: Implementation of minimum cybersecurity standards, including systems designed to recover material financial transactions following an event and audit trails to detect events, the institution of appropriate access privileges, procedures for evaluating and testing the security of applications, multifactor authentication, data disposal, mandatory cybersecurity awareness training, and encryption measures.
6. *Third-Party Risk Management*: Implementation of a third-party risk management program, including a review of the cybersecurity practices of those providers and periodic assessment and audit thereof.

These new requirements, which are the first of their kind, signal an increased focus on risk-prioritized and managed cybersecurity.

Save the Date: On April 4, the article's authors will lead a discussion in Venable's New York City office concerning conducting cybersecurity due diligence in M&A deals. Sellers and purchasers subject to this regulation should consider such due diligence an important aspect of maintaining an appropriate cybersecurity

program. Please email tfacey@Venable.com for more information on the program.

Related Services

Practices

Banking and Financial Services Regulatory

Risk and Compliance (RCOM)

Industries

Cybersecurity Services

eCommerce and Privacy

Financial Services

Related Insights

Consumer Financial Services Practice Digest

3min

November 26, 2019

Significant changes to the federal

3min

regulatory process, new cybersecurity requirements for New York financial institutions, and more in this issue of *Business News Digest*

March 2017

New disguised sale and partnership liability regulations, proposed mandatory cybersecurity regulations, and more in this issue of *Fund Forum*

3min

November 9, 2016

Events

Costa Rica's Recovery From Cyber-Attacks: A Way Forward

August 18, 2022 - Venable LLP, Trend Micro, and Amazon Web Services (AWS)

Women's Equality Day Celebration

August 25, 2022 - New York - WISE+ (Women+ in Samsung Electronics)

Buy Now Pay Later

September 22, 2022 - ETA Fintech Policy Forum

Recent News

Daily Record Recognizes AJ Lynn Among Its 2022 Leading Women

1min

August 18, 2022

The Best Lawyers in America 2023 Recognizes 226 Venable Attorneys

5min

August 18, 2022

Profiles in Diversity Journal Recognizes Belinda Vega Among 2022 Latino Leaders Worth Watching

2min

August 16, 2022

LEXOLOGY

New York Financial Regulator Brings First AML and Cybersecurity Enforcement Action against Licensed Crypto Trading Entity

Blog Blockchain and the Law

Proskauer Rose LLP

USA August 11 2022

In what is the New York Department of Financial Services' (NYDFS) first enforcement action against a NYDFS-licensed "virtual currency business," on August 1, 2022, the agency announced $30 million settlement with cryptocurrency investing platform Robinhood Crypto, LLC ("RHC"). The settlement addressed charges stemming from what the **NYDFS** cited as various deficiencies during 2019-20 of RHC's Bank Secrecy Act (BSA) and anti-money laundering (AML) program and RHS' **cybersecurity** obligations under the agency's Virtual Currency "BitLicense" regulation (23 NYCRR Part 200) and **Cybersecurity** Regulation (23 NYCRR Part 500), among other things

NYDFS has been active in crypto regulation for many years. In 2015, New York was the first state to promulgate a comprehensive framework for regulating virtual currency-related businesses. The keystones of the BitLicense **regulations** are consumer protection, anti-money laundering compliance and **cybersecurity** rules that are intended to place appropriate "guardrails" around the industry while allowing innovation. In addition, NYDFS's **Cybersecurity** Regulation went into effect in March 2017 and generally requires all covered entities, including licensed virtual currency businesses, to establish and maintain a **cybersecurity** program designed to protect the confidentiality, integrity, and availability of its information systems. Licensed virtual currency companies are subject to the same AML and **cybersecurity regulations** as traditional financial services companies.

In 2019 the **NYDFS** granted RHC's application for a BitLicense. The BitLicense, along with a New York state money transmitter license also granted at the time, authorized Robinhood Crypto to offer services for buying, selling and storing various cryptocurrencies to New York residents. Overall, **NYDFS** stated that after conducting a supervisory examination and investigation, it found that RHC had "shortcomings in the company's management and oversight of its compliance programs" and that inadequate staffing and resources were devoted to BSA/AML, transaction monitoring and **cybersecurity** compliance commensurate with its growth. As such, the agency found that RHC's programs did not fully address RHC's operational risks, particularly those associated with operating a cryptocurrency trading platform, and that specific policies within the program were not in full compliance with NYDFS's **Cybersecurity** and Virtual Currency Regulations. Under the settlement, beyond the $30 million penalty, RHC will be required to retain an independent consultant to perform a comprehensive evaluation of the RHC's remediation and compliance efforts.

This is an active summer at **NYDFS** for crypto developments. The RHC settlement follows on the heels of last month's release of a stablecoin guidance meant to set foundational criteria for USD-backed stablecoins issued by

DFS-regulated entities on the issues of redeemability, assets reserves and attestations about such reserves.

Proskauer Rose LLP - Seetha Ramachandran and Jonathan Mollod

Powered by
LEXOLOGY.

$1.8 million penalty issued to financial services firms, signaling increased enforcement of NYDFS cybersecurity regulations

Jul 28, 2021

By: Tom Wojcinski

In April 2021, the New York Department of Financial Services (NYDFS) announced it levied a fine against First Unum Life Insurance Company and Paul Revere Life Insurance Company for violations of NYDFS's Cybersecurity Regulations. The companies are subject to a $1.8 million penalty for failure to comply.
According to the announcement, First Unum and Paul Revere experienced phishing attacks in 2018 and 2019 that compromised the email accounts of several employees — employees who had access to a significant amount of personal and sensitive customer data.

A subsequent investigation found the companies hadn't implemented multi-factor authentication (MFA) or reasonably equivalent access controls. Moreover, the companies falsely certified compliance with the regulations in 2018 when MFA was not fully implemented.

This is just one of several recent NYDFS enforcement actions under the regulations, including a $3 million penalty against National Securities Corporation and $1.5 million against Residential Mortgage Services.

Be aware the effective date for these regulations is well past. If your organization hasn't already been taking these rules seriously, it's time to act — because the regulators certainly are.

Far-reaching cybersecurity regulation

New York's cybersecurity regulation is probably the nation's most comprehensive (some will say "onerous") cybersecurity regulation directed at the financial services industry.

The rules, Cybersecurity Requirements for Financial Services Companies, became effective on March 1, 2017, with a transition period for select requirements; full compliance was expected as of March 1, 2019.

The regulations require all covered entities to adopt a cybersecurity program and meet a minimum cybersecurity standard to protect confidentiality, integrity and availability of a covered entity's information systems.

Under the regulations, a cybersecurity program must perform six core functions:

1. Identify and assess internal cybersecurity risks that threaten security of non-public information maintained by the institution
2. Implement defensive infrastructure, policies and procedures to protect information systems and nonpublic information from unauthorized access or malicious acts
3. Detect cybersecurity events
4. Respond to identified or detected cybersecurity events and mitigate negative effects
5. Recover from cybersecurity events and restore normal operations
6. Fulfill applicable regulatory reporting obligations

Covered entities were required to submit certification of compliance to the superintendent effective February 15, 2018. Further, covered entities need to provide the NYDFS superintendent with all documentation and information relevant to their cybersecurity program upon request.

Does this apply to your financial services firm? Probably.

Under the regulations, a covered entity is defined as those "operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law" of New York. Generally, this would include any business selling a financial services product to customers who are residents of New York.

The following organizations can claim a limited exemption:

- Organizations employing fewer than 10 employees, including independent contractors
- Organizations with gross annual revenue from New York business operations of less than $5 million in each of the last three years

- Organizations with year-end total assets less than $10 million

Even if you meet the exemption, you are still subject to a variety of cybersecurity, risk assessment, access privileges and other requirements.

Your reminder to take action

NYDFS's recent regulatory actions are a reminder to make sure your cybersecurity program is compliant. Businesses are advised to work with a qualified cybersecurity practitioner to verify your organization meets the following requirements:

- Cyber program and risk assessment
- Penetration testing and vulnerability assessments
- Audit trails
- Access privileges
- Application security
- Risk assessment
- Cybersecurity personnel and intelligence
- Third-party service provider security policy
- MFA
- Limitations on data retention
- Training and monitoring
- Encryption of nonpublic information
- Incident response plan
- Notification process

It's important that you have an ongoing audit process to verify compliance and drive corrective action.

Seek expertise to complement your internal team and provide independent perspective on key areas such as CISO, risk assessment, penetration testing and MFA implementation.

Be sure your incident response plan is ready and activated when necessary. Organizations should test and update their plan to be sure they're ready to respond — and defend their actions to the NYDFS — when an incident occurs. (Emphasis on when, not if.)

Covered entities should take recent NYDFS enforcement actions as a sign to take these regulations seriously. Be sure to investigate cybersecurity events, notify NYDFS when required and conduct ongoing risk assessments.

Wipfli can help

Recent NYDFS enforcement actions show just how much companies stand to lose for noncompliance. Wipfli can help financial services firms meet regulatory expectations and protect their organization. Our cybersecurity specialists understand the regulatory landscape as well as the business constraints of the financial services industry.

To receive assistance, talk to your relationship manager or reach out to Wipfli's cybersecurity team today.

Related content:

- Multifactor authentication: Why you need it now
- Cybercrime and your money: Banking on human error
- Fighting the wave of coronavirus phishing scams

Author(s)



Tom Wojcinski, CISA, CRISC
Principal
View Profile

AI

Cybersecurity in 2022 – A Fresh Look at Some Very Alarming Stats

Chuck Brooks Contributor
Global Thought Leader in Cybersecurity and Emerging Tech

Follow

Jan 21, 2022, 05:25pm EST

Listen to article 23 minutes

New!
Follow this author to stay notified about their latest stories.
Got it!



2022 Text with binary code GETTY

Last year I wrote two FORBES articles* that highlighted some of the more significant cyber statistics associated with our expanding digital ecosystem. In retrospect, 2021 was a very trying year for cybersecurity in so many areas. There were high profile breaches such as Solar Winds, Colonial Pipeline and dozens of others that had major economic and security related

impact. Ransomware came on with a vengeance targeting many small and medium businesses. Perhaps most worrisome was how critical infrastructure and supply chains security weaknesses were targeted and exploited by adversaries at higher rates than in the past. Since it is only January, we are just starting to learn of some of the statistics that certainly will trend in 2022. By reviewing the topics below, we can learn what we need to fortify and bolster in terms of cybersecurity throughout the coming year.

- **Alarming Cybersecurity Stats: What You Need To Know For 2021**

Alarming Cybersecurity Stats: What You Need To Know For 2021 (forbes.com)

- **MORE Alarming Cybersecurity Stats For 2021 !** MORE Alarming Cybersecurity Stats For 2021 ! (forbes.com)

Cybersecurity and Business



Network of business concept. GETTY

MORE FROM FORBES ADVISOR

Best Travel Insurance Companies

By **Amy Danise** Editor

Best Covid-19 Travel Insurance Plans

By **Amy Danise** Editor

The past two years has seen a rapid shift of work to remote and hybrid offices. The statistics show that hackers welcomed that shift and took advantage of the vulnerabilities and gaps in security by businesses.

Cyber risks top worldwide business concerns in 2022 Cyber risks top worldwide business concerns in 2022 - Help Net Security

"Cyber perils are the biggest concern for companies globally in 2022, according to the Allianz Risk Barometer. The threat of ransomware attacks, data breaches or major IT outages worries companies even more than business and supply chain disruption, natural disasters or the COVID-19 pandemic, all of which have heavily affected firms in the past year.

Cyber incidents tops the Allianz Risk Barometer for only the second time in the survey's history (44% of responses), Business interruption drops to a close second (42%) and Natural catastrophes ranks third (25%), up from sixth in 2021. Climate change climbs to its highest-ever ranking of sixth (17%, up from ninth), while Pandemic outbreak drops to fourth (22%).y affected firms in the past year. "

Cybercriminals can penetrate 93 percent of company networks Cybercriminals can penetrate 93 percent of company

networks (betanews.com)

“among the findings of a new study of pentesting projects from Positive Technologies, conducted among financial organizations, fuel and energy organizations, government bodies, industrial businesses, IT companies and other sectors. In 93 percent of cases, an external attacker can breach an organization's network perimeter and gain access to local network resources.”

Businesses Suffered 50% More Cyberattack Attempts per Week in 2021 Businesses Suffered 50% More Cyberattack Attempts per Week in 2021 (darkreading.com)

The rise — partly due to Log4j — helped boost cyberattack attempts to an all-time high in Q4 2021, new data shows. The education/research sector sustained the most attacks in 2021, followed by government/military and communications. Source: Check Point Software



thumbnail (2) CHECKPOINT

Corporate Cyber Attacks Up 50% Last Year

Corporate Cyber Attacks Up 50% Last Year (cybersecurityintelligence.com)

2021 saw 50% more cyber attacks per week on corporate networks compared to 2020.

Most Targeted Sectors Worldwide by Hackers in 2021

- Education/Research sector up by 75%
- Cyber attacks on Healthcare sector up by 71%
- ISP/MSP up by 67%
- Communications +51%
- Government / Military sector up by 47%

Cybersecurity and Small and Medium Sized Businesses

While many large businesses suffered breaches, small and medium businesses were an easier target for hackers because of their lack of resources and security expertise.

2022 Must-Know Cyber Attack Statistics and Trends
2021 Must-Know Cyber Attack Statistics and Trends - Embroker

Cyber attacks on all businesses, but particularly small to medium sized businesses, are becoming more frequent, targeted, and complex. According to Accenture's Cost of Cybercrime Study, 43% of cyber attacks are aimed at small businesses, but only 14% are prepared to defend themselves.

Not only does a cyber attack disrupt normal operations, but it

may cause damage to important IT assets and infrastructure that can be impossible to recover from without the budget or resources to do so.

Small businesses struggling to defend themselves because of this. According to Ponemon Institute's State of Cybersecurity Report, small to medium sized business around the globe report recent experiences with cyber attacks:

- **Insufficient security measures**: 45% say that their processes are ineffective at mitigating attacks.
- **Frequency of attacks**: 66% have experienced a cyber attack in the past 12 months.
- **Background of attacks**: 69% say that cyber attacks are becoming more targeted.

The most common types of attacks on small businesses include:

- **Phishing/Social Engineering**: 57%
- **Compromised/Stolen Devices**: 33%
- **Credential Theft**: 30%

10 Small Business Cyber Security Statistics That You Should Know – And How To Improve Them 10 Small Business Cyber Security Statistics That You Should Know – And How To Improve Them - Cybersecurity Magazine (cybersecurity-magazine.com)

"Keeping up with the latest cyber-attack statistics is pertinent for understanding the state of cyber threats, commonly leveraged vulnerabilities, implications of successful cyber attacks, and effective strategies for mitigating prevalent threats.

1. 43% of all data breaches involve small and medium-sized businesses.
2. If you're still in denial about the chances of your small business becoming a victim, 61% of all SMBs have reported at least one cyber attack during the previous year.
3. A benchmark study by CISCO found that 40% of the small businesses that faced a severe cyber attack experienced at least eight hours of downtime. And this downtime accounts for a major portion of the overall cost of a security breach.
4. The above-mentioned CISCO study also found that ransomware was not among the top three cyber threats identified by small businesses. Business owners may be underestimating the threat of ransomware, however, MSPs are not. 85% of MSPs consider ransomware one of the biggest threats to their SMB clients.
5. 30% of small businesses consider phishing attacks to be the biggest cyber threat.
6. 83% of small and medium-sized businesses are not financially prepared to recover from a cyber attack.
7. Despite the staggering numbers, 91% of small businesses haven't purchased cyber liability insurance. This truly reflects how unaware and unprepared small business owners are to deal with security breaches.
8. Only 14% of small businesses consider their cyber attack and risk mitigation ability as highly effective.
9. 43% SMBs do not have any cybersecurity plan in place.
10. One in five small companies does not use endpoint security, and 52% SMBs do not have any IT security experts in-house."

Cybersecurity and Healthcare:



The concept of innovative information technology in medicine. GETTY

Most hospitals and healthcare facilities have traditionally focused their budgets on acquiring new medical technologies and improving patient care. Covid19 put a huge burden on budgets and hackers have exploited cyber vulnerabilities, especially via ransomware.

Healthcare Cybersecurity Report 2021-2022 Healthcare Cybersecurity Report 2021-2022 (herjavecgroup.com)

"70% of recently surveyed organizations reported that healthcare ransomware attacks have resulted in longer lengths of stays in hospital and delays in procedures and tests that have resulted in poor outcomes including an increase in patient mortality."

Half of internet-connected devices in hospitals are vulnerable to hacks, report finds Half of internet-connected devices in hospitals are vulnerable to hacks, report finds - The Verge

"Over half of internet-connected devices used in hospitals have a vulnerability that could put patient safety, confidential data, or

the usability of a device at risk, according to a new report from the healthcare cybersecurity company Cynerio.

The report analyzed data from over 10 million devices at over 300 hospitals and health care facilities globally, which the company collected through connectors attached to the devices as part of its security platform."

Cybersecurity and IoT Devices:

With everything and anything connected, hackers can take advantage of many attack vectors and weak device passwords. The threat is growing as IoT expands.

Top 10 cyber security threats in 2021 List secondary lists page (cybermagazine.com)

According to Symantec, IoT devices experience an average 5,200 attacks per month. The fact that a majority of new IoT devices are still in their infancy means there is a much larger attack surface for cybercriminals to target the vulnerabilities associated with them.

For a deep dive on the IoT Cybersecurity conundrum, Please see my slide below and FORBES article: **Cybersecurity Threats: The Daunting Challenge of Securing the Internet Of Things**: Cybersecurity Threats: The Daunting Challenge Of Securing The Internet Of Things (forbes.com)



IoT Cyber Vulnerabilities CHUCK BROOKS

Ransomware:

Although ransomware has been around for decades, in 2021 it became a preferred cyber-weapon of choice for hackers. Being able to exfiltrate and hold hostage data for payment of cryptocurrencies has made the deployment of ransomware a growing trend.

Ransomware Statistics, Trends and Facts for 2022 and Beyond Ransomware Statistics, Trends and Facts for 2022 and Beyond (cloudwards.net)

5 Key Ransomware Statistics:

1. Ransomware cost the world **$20 billion in 2021**. That number is expected to rise to **$265 billion by 2031**.
2. In 2021, **37 percent of all businesses and organizations** were hit by ransomware.

3. Recovering from a ransomware attack cost businesses **$1.85 million on average in 2021**.
4. Out of all ransomware victims, **32 percent pay the ransom**, but they only **get 65 percent of their data back**.
5. Only **57 percent of businesses** are successful in recovering their data using a backup.



Ransomware by the Numbers CLOUDWARDS

Please also see my recent FORBES article:

Ransomware on a Rampage; a New Wake-Up Call
Ransomware on a Rampage; a New Wake-Up Call (forbes.com)

“The sobering reality is that ransomware is on a rampage.

Ransomware will continue to be a destructive threat because there are so many available soft targets. We live in an increasingly hyper-connected world that impacts all aspects of our lives. From now and onward, managing and protecting data will be a security imperative for every industry and organization.

Awareness and understanding the ransomware threat can help address many of the cybersecurity challenges. Emerging cybersecurity technologies, mitigation tools, and protocols can help limit the exploding trend of ransomware attacks. Taking pro-active measures to protect systems, networks, and devices, and be more resilient, need to be part of a new wake-up call."

Compendiums On Cybersecurity Statistics:



global communication network concept GETTY

If you seek a more comprehensive overview of cybersecurity stats, please check out these compendium articles. They cover many policy, operational, and industry specific elements of the

cybersecurity ecosystem.

- 2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics 2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics (cybersecurityventures.com)t is estimated that an organization suffered a ransomware attack every 11 seconds in 2021, according to Cybersecurity Ventures, and it is expected there will be a new attack on a consumer or business every two seconds by 2031.

CRYPTOCRIME

- Cryptocrime, or crimes having to do with cryptocurrencies, are predicted to exceed $30 billion in 2025, up from an estimated $17.5 billion in 2021, according to Cybersecurity Ventures.

CYBERSECURITY SPENDING

- The imperative to protect increasingly digitized businesses, Internet of Things (IoT) devices, and consumers from cybercrime will propel global spending on cybersecurity products and services to $1.75 trillion cumulatively for the five-year period from 2021 to 2025, according to Cybersecurity Ventures, up from $1 trillion cumulatively from 2017 to 2021.

VENTURE CAPITAL

- Cybersecurity Ventures tracked more than $23 billion in venture capital devoted to cybersecurity companies in 2021.

Cybersecurity Ventures Infographic:



Cybersecurity-Almanac-2022-Infographic-1536x1151 CYBERSECURITY VENTURES

All the Cybersecurity Statistics, Figures and Facts You Need to Know in 2022

All the Cybersecurity Statistics, Figures and Facts You Need to Know in 2022 | Cybersecurity | CompTIA

"State Sponsored Threats: According to Microsoft, nearly 80% of nation-state attackers targeted government agencies, thinks tanks and other non-government organizations.

The United States remains the most highly targeted country with 46% of global cyberattacks being directed towards Americans

Cost of Cybercrime rising: The cost of cyber crime has risen 10% in the past year.

Cybersecurity Workforce: it's estimated that there will be 3.5 million unfilled cybersecurity jobs by the end of 2025.

The pandemic presented lots of new cybersecurity issues and companies are working diligently to ensure they are prepared for anything that comes their way in the future. Expect to see the following.

· Enhanced software supply chain security.

· Ransomware will become more of a problem for businesses.

· Companies are transitioning to a zero trust framework for cybersecurity.

· Increased scrutiny on the cybersecurity measures of third-party providers.

· Rise in cyber insurance to offer further protection for businesses."

22 Cyberstatistics to Know for 2022 22 cybersecurity statistics to know for 2022 | WeLiveSecurity

Phishing Attacks: Phishing attacks were connected to 36% of breaches, an increase of 11%, which in part could be attributed to the COVID-19 pandemic. As might have been expected, threat actors have been observed tweaking their phishing campaigns based on what's making the news at any moment in time. (Verizon 2021 Data Breach Investigations Report)

Cost of Data Breach: 2021 saw the highest average cost of a data breach in 17 years, with the cost rising from US$3.86 million

to US$4.24 million on an annual basis. (IBM Cost of a Data Breach Report 2021)

Ransomware Payouts: Cryptocurrency has been the preferred payment method for cybercriminals for a while now, especially when it comes to ransomware. As much as US$5.2 billion worth of outgoing Bitcoin transactions may be tied to ransomware payouts involving the top 10 most common ransomware variants. (FinCEN Report on Ransomware Trends in Bank Secrecy Act Data)

DDoS Attacks: The number of distributed denial-of-service (DDoS) attacks has also been on the upward trend, in part due to the COVID-19 pandemic. 2020 saw more than 10 million attacks occur, 1.6 million attacks more than the previous year. (ENISA Threat Landscape 2021)

Cybersecurity Statistics for 2022 (Infographic)

Cybersecurity Statistics for 2022 (Infographic) (judge.com)


95%

Cybersecurity In The Year Ahead



Futuristic city VR wire frame with group of people. This is entirely 3D generated image.
GETTY

The Top 22 Security Predictions for 2022 The Top 22 Security Predictions for 2022 (govtech.com)

Dan Lohrmann is one of the world's most knowledgeable and prolific cybersecurity experts. His article on predications for 2022

"What will the New Year bring in cyber space? Here's your annual roundup of the top security industry forecasts, trends and cybersecurity prediction reports for calendar year 2022.

Last December in "The Top 21 Security Predictions For 2021," I noted the following summary of expected trends for 2021:

- There will be huge security impacts in the coming year from the move to work from home (WFH) fueled by COVID-19. More attacks will occur on home computers and networks, with bad actors even using home offices as criminal hubs by taking advantage of unpatched systems and architecture weaknesses.

- The rush to cloud-everything will cause many security holes, challenges, misconfigurations and outages.
- More growth in the security industry. Our numbers of new products and new mergers and acquisitions will cause network complexity issues and integration problems and overwhelm cyber teams.
- Privacy will be a mess, with user revolts, new laws, confusion and self-regulation failing.
- Identity and multi-factor authentication (MFA) will take center stage as passwords (finally) start to go away in a tipping-point year.
- Tons of high-profile IoT hacks, some of which will make headline news.
- Ransomware will get worse and worse — with new twists, data stealing prior to encryption, malware packaging with other threats and very specific targeting of organizations.
- Lots of 5G vulnerabilities will become headline news as the technology grows.
- Advanced Persistent Threats (APT) attacks will be widely available from criminal networks. The dark web will allow criminals to buy access into more sensitive corporate networks.

New focuses this year cover:

- Cyber threats in space.
- A heavy emphasis on operational technology (OT) cybersecurity — vulnerabilities, threats and impacts.

- A strong emphasis on cryptocurrencies and crypto wallet security attacks. As Bitcoin and other cryptocurrencies rose in 2021, now the bad actors want your bitcoins even more.
- More application security vulnerabilities — especially when code is widely used, such as the Log4j vulnerabilities.
- Issues created by a lack of talent and vacancies in public- and private-sector organizations — as the talent war gets worse.
- Renewed emphasis (but in new ways) on AI, autonomous vehicles, drones and other new technologies being hacked.
- Note that security industry vendor acquisitions have changed many of the familiar names, such as the activities with FireEye, McAfee Enterprise and Mandiant.

Industry expert Chuck Brooks also offered these security predictions for the new year on the AT&T website. Here are two:

- **More automation and visibility tools** will be deployed for expanding protection of remote employee offices, and for alleviating workforce shortages. The automation tools are being bolstered in capabilities by artificial intelligence and machine learning algorithms.
- **Cybersecurity will see increased operational budgets** because of more sophisticated threats and consequences of breaches (and especially ransomware) to the bottom line. Cybersecurity becomes more of a C-Suite issue with every passing year as breaches can be disruptive and devastating for business."

Conclusion:



Road to success concept and sustainable development idea GETTY

I only touched a tiny bit of the topics and issues relating to cybersecurity stats and predictions. Please see my analysis on protecting critical infrastructure and supply chains as we move forward in 2022. It is a large and important challenge! I will revisit new stats later in the year ad cybersecurity is never static.

GovCon Expert Chuck Brooks Highlights Importance of Protecting Critical Infrastructure; Supply Chains in 2022

GovCon Expert Chuck Brooks Highlights Importance of Protecting Critical Infrastructure; Supply Chains in 2022 (executivegov.com)

by William McCormick

GovCon Expert Chuck Brooks, a highly esteemed cybersecurity leader, recently published his latest feature in the January issue of the CISO MAG detailing the importance for federal executives to focus on protecting the critical infrastructure supply chain in IT and OT systems.

“Protecting critical infrastructure Industrial Control Systems, Operational Technology, and IT systems from cybersecurity threats is a difficult endeavor,” said Chuck Brooks. “They all have unique operational frameworks, access points, and a variety of legacy systems and emerging technologies. Protecting the critical infrastructure supply chain in IT and OT systems will be a public and private sector priority.”

In addition, GovCon Expert Chuck Brooks discussed the potential cybersecurity workforce shortage that could exist in 2022. It was reported by Cybersecurity Ventures that roughly 3.5 million jobs in cybersecurity were left unfilled in 2021, which could pose significant operational challenges in the federal sector moving forward.

Brooks mentioned the Internet of Things (IoT) as an area to watch for growing cybersecurity risks. In particular, Brooks highlighted the challenge that IoT poses from having a lack of visibility and the ability to determine if a device has been compromised and not performing as intended.

“The increased integration of endpoints combined with a rapidly growing and poorly controlled attack surface poses a significant threat to the Internet of Things,” Brooks explained. “Protecting such an enormous attack surface is no easy task, especially when there are so many varying types and security standards on the devices. It will only worsen in 2022 as connectivity grows.”

You can read the full article from GovCon Expert Chuck Brooks on CISO MAG.

Author's Bio:

Chuck Brooks, President of Brooks Consulting International, and Adjunct Faculty at Georgetown University. He is a Technology Evangelist, Corporate Executive, Speaker, Writer, Government Relations, and Marketing Executive. LinkedIn named Chuck as one of "The Top 5 Tech People to Follow on LinkedIn." He was named as one of the world's "10 Best Cyber Security and Technology Experts" by Best Rated, as a "Top 50 Global Influencer in Risk, Compliance," by Thomson Reuters, "Best of The Word in Security" by CISO Platform, and by IFSEC as the "#2 Global Cybersecurity Influencer." He was featured in the 2020 and 2021 Onalytica "Who's Who in Cybersecurity" – as one of the top Influencers for cybersecurity issues and in Risk management. He was also named "Best in The World in Security" by CISO Platform, one of the "Top 5 Executives to Follow on Cybersecurity" by Executive Mosaic, and as a "Top Leader in Cybersecurity and Emerging Technologies" by Thinkers360. Chuck was named by Oncon in 2019 "Top Global Top 50 Marketer" by his peers across industry.

Chuck also a Cybersecurity Expert for "The Network" at the Washington Post, Visiting Editor at Homeland Security Today, Expert for Executive Mosaic/GovCon, the Advisory Board of CISO MAG, and a Contributor to FORBES. He has a BA from DePauw University, and MA from the University of Chicago, and studied at the Hague Academy of International Law

Follow me on Twitter or LinkedIn. Check out my website.



Chuck Brooks

Follow

Chuck Brooks, President of Brooks Consulting International, is a globally recognized thought leader and subject matter expert Cybersecurity and Emerging... **Read More**

Editorial Standards

Reprints & Permissions