10 Commandments of Cybersecurity for Lawyers

Speakers:

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

Scott James Shackelford, Professor of Law, Cybersecurity Program Chair, Indiana University Bloomington

Siobhan Gorman, Partner, Brunswick Group

(c) 2021 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) 2021 Lexeprint Inc. All Rights Reserved



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



Scott James Shackelford
Professor of Law, Cybersecurity
Program Chair, Indiana
University Bloomington



Siobhan Gorman
Partner, Brunswick Group

(c) 2021 Lexeprint Inc. All Rights Reserved

Agenda

1

Cybersecurity Priorities to Pay Attention to in 2021

2

Ten Commandments of Cybersecurity

3

Recent Cyber Incidents

(c) 2021 Lexeprint Inc. All Rights Reserved



Cybersecurity Priorities to Pay Attention to in 2021

(c) 2021 Lexeprint Inc. All Rights Reserved



The Cybersecurity Backdrop

- The average global cost of a data breach is $3.86 million (IBM Cost of Data Breach).
  - According to the same study, the US has the highest average of any country at $8.64 million.
  - The healthcare industry faces the highest costs overall.
- In 2019, it was estimated that a business fell victim to a cyber attack every 14 seconds (2019 Official Annual Cybercrime Report).

(c) 2021 Lexeprint Inc. All Rights Reserved



Nation-State Actors

- Destructive attacks and attempts can be expected in 2021 as geopolitical tensions are on the rise.
- The former Director of National Intelligence, Daniel Coats listed cybersecurity as the top global threat. He also noted that it is very probable that every U.S. foreign adversary would try to undermine American infrastructures through cyber-attacks and influence operations.
- It will be crucial to implement security measures to defend against these ongoing threats as nation-state actors will only continue trying new tactics to profit and sow discourse.

(c) 2021 Lexeprint Inc. All Rights Reserved



Ransomware Payments

- OFAC has said that "companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations."

(c) 2021 Lexeprint Inc. All Rights Reserved



New Concerns that Ransomware Payments May Violate US Sanctions

- Companies facing extortion demands from cybercriminals have encountered a new form of risk in recent months over whether paying such a ransom could violate sanctions issued by the U.S. Department of the Treasury.
- This follows a cyberattack on wearable technology company, Garmin Ltd., where malicious software knocked service offline for users of its fitness tracking products.
- Garmin has not said whether it paid a ransom. But a news report said the company used an intermediary to pay a multimillion-dollar bounty to criminals who had hit its network with a virus known as "WastedLocker," which some cybersecurity experts say was developed by a Russia-based, sanctioned cybercriminal group that calls itself "Evil Corp."
- The Treasury's Office of Foreign Assets Control, or OFAC, has yet to penalize a U.S. entity for making a payment to a group of cybercriminals under sanction.

(c) 2021 Lexeprint Inc. All Rights Reserved



COVID-19 Pandemic

- The onset of the coronavirus pandemic has completely altered the world, but unfortunately cyber criminals have not ceased their attacks.
- Instead, they are exploiting vulnerabilities created by the large number of persons working at home and launching attacks on medical facilities.

(c) 2021 Lexeprint Inc. All Rights Reserved



Work from Home Can Lead to Increased Vulnerability

- In a survey published by the CNBC Technology Executive Council, 36 percent of executives reported an increase in cyber threats as the majority of their employees have shifted to working from home.
- The survey noted that 85 percent of senior technology executives had at least half of their employees working from home; 25 percent of those surveyed were fully remote.

(c) 2021 Lexeprint Inc. All Rights Reserved



Work from Home Can Lead to Increased Vulnerability (cont.)

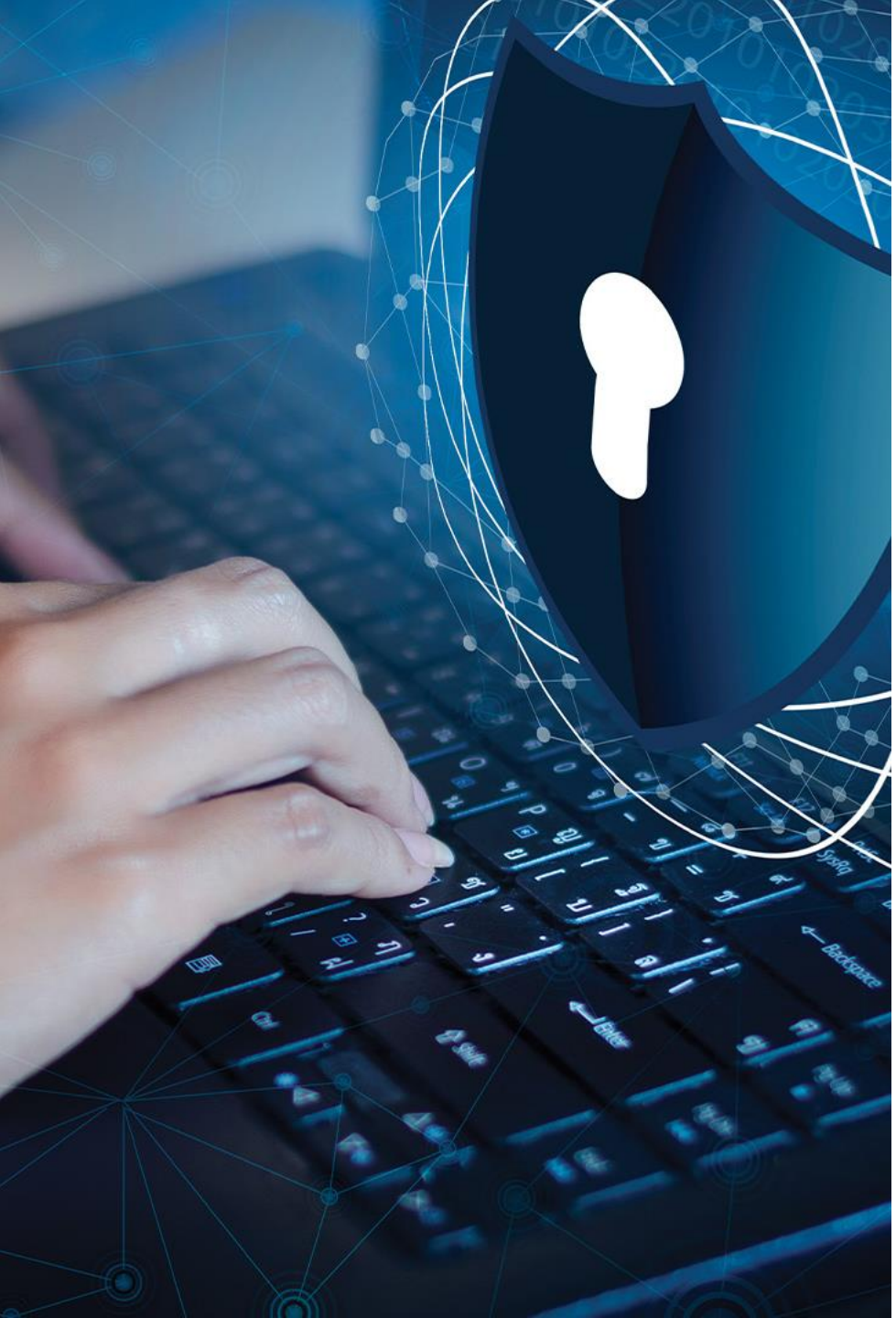
- As the coronavirus is causing more employees to work remotely, it is possible that those individuals are logging in remotely from a less secure network and perhaps using less secure hardware.
- High volumes of employees logging in remotely may make it easier for cyber criminals, infiltrating a network through remote desktop services, to stay hidden in an attempt to identify and access systems with sensitive data.

(c) 2021 Lexeprint Inc. All Rights Reserved



10 Commandments of Cybersecurity

(c) 2021 Lexeprint Inc. All Rights Reserved



First Commandment

Develop and Practice Strong Cyber Hygiene

- Implement robust passwords or other advanced means of authentication
- Ensure security of computing and communication devices, especially when travelling abroad
- Train all employees on proper email etiquette
- Increase and demonstrate cybersecurity common sense as part of performance reviews
- Utilize surveillance and malware detonation software
- Assess the security needs for encrypted phones, laptops and smart devices

(c) 2021 Lexeprint Inc. All Rights Reserved


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

Second Commandment
Know and Secure Your Vendors

- Limit access in accordance to need
- Review existing contact language: Understand vendors' cybersecurity protocols
- Contractually bind vendors to security standards and protocols
- Identify, rank, engage, and audit third-party vendors in accordance with geography and business importance and remember that good vendors are partners
- Require vendors that provide critical data to disclose cyber incidents within 72 hours of occurrence

(c) 2021 Lexeprint Inc. All Rights Reserved



Third Commandment

Identify and Insure “Crown Jewels”

- Identify and segregate critical data and systems
- Verify and update processes with business stakeholders, including C-suite and board
- Implement and continually update appropriate controls, systems, and processes to protect systems
- Ensure the continued protection of critical data in the most effective manner

(c) 2021 Lexeprint Inc. All Rights Reserved



Fourth Commandment

Develop an Incident Response Plan

- Engage all key components (business, legal, marketing, insurance, HR, IT) to develop a cross-functional incident response plan and team
- Retain outside technical, legal and PR experts for the inevitable cyber incident
- Identify points of contact within law enforcement before a cyber-attack
- Focus on range, motivations and objectives of potential attacks (theft, denial of service, ransom, publication)
- Compliance with privacy laws and focus on protection of the confidentiality of the work

(c) 2021 Lexeprint Inc. All Rights Reserved



Fifth Commandment

Create and Develop a Global Communications and Messaging Framework

- Communications plan covers:
  - Employees, consumers, customers, regulators, and investors
  - Appropriate regulators that will expect disclosure identified
  - Media, social media and source-channels for disseminating company information identified
  - Messaging experts to ensure a coordinated response when it is needed, retained

(c) 2021 Lexeprint Inc. All Rights Reserved



Sixth Commandment

Test the Incident Response Plan Regularly

- Third Party Testing
  - Utilize a third-party firm to conduct annual penetration tests to identify weaknesses in IT networks, infrastructure and employee practices
- Disclose Results to Board
  - Report the results to the board and C-suite on a regular basis
- Hire Cyber Threat Intelligence
  - Engage a third-party to monitor the Internet and dark web for stolen data and information on key executives and business operations

(c) 2021 Lexeprint Inc. All Rights Reserved



Seventh Commandment

Develop a Robust Cyber-Threat Monitoring Platform and Response Team

- Monitor cyber-threats internally and externally, and probe systems
- Drill/test employee practices and compliance
- Participate in industry cyber-threat sharing platforms, and ensure an organization ability to act on the intelligence provided

(c) 2021 Lexeprint Inc. All Rights Reserved



Eighth Commandment

Evaluate and Purchase Cybersecurity Insurance

- Assess the full range of risks and costs from disruption of services, data leaks, data ransoms and extortion schemes
- Verify and validate that key partners have coverage: a vendor that is hacked can lead to your organization being compromised
- Ensure that coverages map to the cybersecurity controls, process, vendors and protocols in any incident- response plan.
- Stay abreast of the market: Cyber Insurance is still evolving, coverage and pricing are in progress
- Policies and available products must be continuously viewed for gaps, newly available coverage and price-competitiveness

(c) 2021 Lexeprint Inc. All Rights Reserved



Ninth Commandment

Meet and Greet Privacy and Cybersecurity Expertise in All Priority Jurisdictions

- Compile industry contacts list of information and threat sharing
- Petition government for assistance, and liability safe harbors where appropriate
- Maintained and updated on a regular basis
- Consult privacy counsel to ensure that cybersecurity solutions do not violate local laws

(c) 2021 Lexeprint Inc. All Rights Reserved



Tenth Commandment

Review Your Contracts with Clients

- Access to Clients networks and systems if access is necessary in connection with responding to a breach.
- Notification requirements to provide and receive and that they are appropriate in context of the relationship
- Insurance coverage in case of a breach and to ensure that you have coverage and vice versa.

(c) 2021 Lexeprint Inc. All Rights Reserved



Recent Cyber Incidents

(c) 2021 Lexeprint Inc. All Rights Reserved



FireEye

- In December 2020, FireEye, one of the world's largest security firms, disclosed a cybersecurity breach.
  - A nation-state group is suspected behind the attack.
- FireEye explained that a "highly sophisticated threat actor" accessed its internal network and stole hacking tools the company uses to test the networks of its customers.
- It is believed that around 18,000 organizations had the malicious code in their networks, and that 50 firms suffered major breaches.

(c) 2021 Lexeprint Inc. All Rights Reserved



Beaumont Health

- In April 2020, the personal and medical information of over 112,000 employees and patients of Beaumont Health was accessed by a malicious actor after compromising employee email accounts through a phishing attack.
- The information impacted includes names, birth dates, Social Security numbers, driver's license numbers, medical condition data, and bank account data.
- In June 2020, Beaumont announced that the data of another 6,000 patients following another phishing attack.
    - Emails contained personal information that included names, dates of birth, diagnoses, diagnosis codes, procedure and treatment information, type of treatment provided, prescription information, patient account numbers, and medical record numbers.

(c) 2021 Lexeprint Inc. All Rights Reserved



Facebook

- In April 2020, more than 267 million Facebook profiles were listed for sale on the Dark Web – all for $540.
- These profiles link to a data leak discovered in December 2019, with additional PII attached, including email addresses, names, Facebook IDs, dates of birth, and phone numbers.
- It is unclear how the data was originally exposed.

(c) 2021 Lexeprint Inc. All Rights Reserved



Questions?

(c) 2021 Lexeprint Inc. All Rights Reserved

Contact Us



Daniel B. Garrie
Phone: 855-529-2466
Email: daniel@lawandforensics.com
URL: www.lawandforensics.com



Scott James Shackelford
Phone: (812) 856-6728
Email: sjshacke@indiana.edu
URL: https://law.indiana.edu



Siobhan Gorman
Phone: (202) 374-9781
Email: sgorman@brunswickgroup.com
URL: https://www.brunswickgroup.com

(c) 2021 Lexeprint Inc. All Rights Reserved



Daniel B. Garrie, Esq.
Law & Forensics – Co-founder
JAMS – Mediator, Arbitrator, eDiscovery Special Master
Contact:
W: (855) 529-2466
E: daniel@lawandforensics.com
URL: 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 is the Co-Founder of Law & Forensics LLC, Head of Computer Forensics and Cyber Security Practice Groups and has been a dominant voice in the computer forensic and cybersecurity space for over 20 years. Prior to Daniel's legal career, 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. Daniel has both a Bachelor's and a Master's Degree in computer science from Brandeis University, as well as a J.D. degree from Rutgers Law School. Daniel has led forensic teams in some of the most visible and sensitive cyber incidents in the United States. In particular, Daniel recently located and recovered deleted files in both private and public cloud computing environments using his patented software, Forensic Scan. This investigation took less than forty-eight hours to clean and recover the data from the servers of a cloud-hosting provider that was compromised by a malicious cyber-attack. Thanks to the Forensic Scan technology, that Daniel co-invented and patented (US9990498B2 and US9990497B2), and his own expertise, Daniel and his team was able to identify the source of the breach and remediate the problem in record time.

Daniel regularly testifies as an e-discovery, cybersecurity and computer forensic expert witness, authoring forensic expert reports on multi-million-dollar disputes. His ability to perform complex investigations and effectively communicate the results to a jury has made him one of the most sought-after experts in the country. His testimony has been pivotal in a number of cases, including one involving the embezzlement of millions of dollars from a large non-profit. Daniel was able to perform a thorough analysis of the alleged embezzlers' phone and computer, despite the embezzlers' attempts to wipe them, and identify concrete evidence of the embezzlement to a jury. Since 2008, Daniel has served as a Neutral and Special Master and in 2016, he joined JAMS as one of the organization's youngest Neutrals. At JAMS, Daniel serves as an Arbitrator, Forensic Neutral, and technical Special Master with a focus on cybersecurity, cyrptocurrency, and complex software and technology related disputes. Some of the major cases for which he has served as an e-discovery special master, or forensic neutral include: *Hougan vs. City of Newport Beach, No. 30-2012-00582855* (Super. Ct. Cal. 2014)*; Small v. University Medical Center of Southern Nevada, 2014 WL 4079507*(D. Nev. 2014)*; C.D.S. Inc. v. Zelter and Amazon Web Services, Inc.*, (S.D.N.Y. 2016); *Jawbone, Inc. v. Fitbit Inc.* et al (Super. Cal., S.F. County 2018). In addition to his vast litigious experience, Daniel is well-published in the cybersecurity space, Editor-in-Chief of the Journal of Law & Cyberwarfare, author of more than 200 articles and books including, "Understanding Software, the Internet, Mobile Computing, and the Cloud. A guide for Judges", published by the Federal Judicial Center. He has been recognized by several United States Supreme Court Justices for his legal scholarship and is a trusted source and a thought leader for cybersecurity articles and opinions, being cited over 500 times to date.

(c) 2021 Lexeprint Inc. All Rights Reserved



Scott James Shackelford
Indiana University Bloomington – Professor of Law, Cybersecurity Program Chair
Contact:
E: sjshacke@indiana.edu
W: (812) 856-6728
URL: https://law.indiana.edu

Professor Scott J. Shackelford serves on the faculty of Indiana University, where he is cybersecurity program chair and director of the Ostrom Workshop Program on Cybersecurity and Internet Governance. He is also an affiliated scholar at both the Harvard Kennedy School's Belfer Center for Science and International Affairs and Stanford's Center for Internet and Society, as well as a senior fellow at the Center for Applied Cybersecurity Research, and a term member at the Council on Foreign Relations.

Shackelford has written more than 100 articles, book chapters, essays, and op-eds for diverse outlets ranging from the University of Illinois Law Review and the American Business Law Journal to the Christian Science Monitor, Huffington Post, Slate, The Conversation, and the San Francisco Chronicle. Similarly, his research has been covered by diverse outlets, including Politico, NPR, Marketplace, Forbes, Time, Associated Press, Forensics Magazine, Law360, the Indianapolis Star, Washington Post, and the Los Angeles Times. He is also the author of Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace (Cambridge University Press, 2014).

Both Shackelford's academic work and teaching have been recognized with numerous awards, including a Harvard University Research Fellowship, a Stanford University Hoover Institution National Fellowship, a Notre Dame Institute for Advanced Study Distinguished Fellowship, the 2014 Indiana University Outstanding Junior Faculty Award, and the 2015 Elinor Ostrom Award.

(c) 2021 Lexeprint Inc. All Rights Reserved



Siobhan Gorman
Brunswick Group – Partner
Contact:
E: sgorman@brunswickgroup.com
W: (202) 374-9781
URL: https://www.brunswickgroup.com

BRUNSWICK

Siobhan Gorman is a Partner in Brunswick's Washington, DC office, where she concentrates on crisis, cybersecurity, public affairs, and media relations.

As a co-chair of the global Cybersecurity and Privacy practice, Siobhan has also led a range of cybersecurity, public affairs, litigation, and corporate reputation projects in the financial, retail, airline, and technology sectors. Siobhan has advised a range of companies on cyber preparedness and response issues, including Delta Air Lines, Southwest Airlines, Under Armour, Hiscox, HBO, and Accenture Federal Services. She is a member of the Senior Advisory Group for Harvard University's Defending Digital Democracy Project, which is focused on preventing and mitigating cyberattacks on the election process, and she has advised state and local election officials around the country on cyber crisis management. She is also member of the Advisory Committee for Brown University's Executive Master in Cybersecurity. Last year, Siobhan hosted a weekly consumer cybersecurity segment on local CBS stations, called "Eye on Cyber."

Prior to joining Brunswick, Siobhan had a successful 17-year career as a reporter, most recently at The Wall Street Journal. At The Journal, she covered a range of national security and law enforcement topics, including counterterrorism, intelligence, and cybersecurity. She has been nominated three times for the Pulitzer Prize.

(c) 2021 Lexeprint Inc. All Rights Reserved