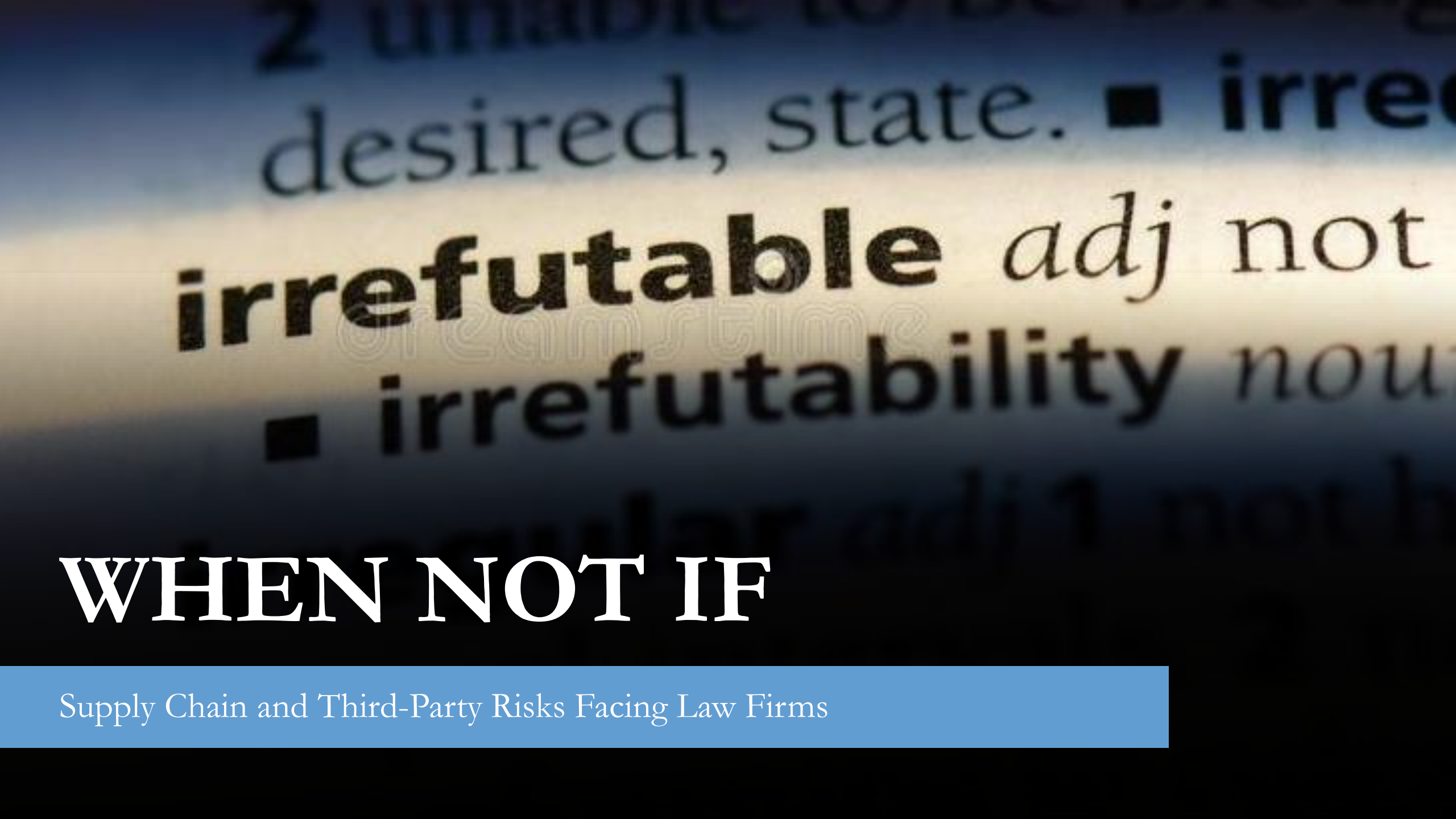
the 20TH ANNUAL LAW FIRM COO AND CFO FORUM

Breakout 4:
Stir of Echoes: Law Firm Lessons from the SolarWinds Hack

David Cass
Vice President – Cyber & IT Risk,
Federal Reserve Bank of New York

Daniel B. Garrie, Esq.
Co-Founder,
Law & Forensics LLC



WHEN NOT IF

Supply Chain and Third-Party Risks Facing Law Firms

Law Firms Today

- Decentralized structure
- Client requirements
- Executive orders, State law, Regulators, and Federal law
- Ethical Guidelines

Copyright © 2021. Law & Forensics. Privileged & Confidential. Not for distribution or publication.

Executive Order 14028 Signed 05/12/2021

"The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy….The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace."

Copyright © 2021. Law & Forensics. Privileged & Confidential. Not for distribution or publication.

The Numbers

- According to PwC Law Firm's Survey 2020, cyber risk is the second greatest threat to law firms from now until 2022 after Covid-19.
- An ABA Report from 2020 showed that 29% of law firms reported a security breach, and 36% reported malware infections
- 71% of the Top 100 firms said they were "somewhat concerned" or "extremely concerned" about cybersecurity threats
- **The problem is, only 22% of Top 100 firms have a Cybersecurity Committee**

Copyright © 2021. Law & Forensics. Privileged & Confidential. Not for distribution or publication.

Why Law Firms?

- Law firms have become increasingly more vulnerable to cyber attacks
- They are enticing to cyber criminals because they handle and store sensitive and confidential data as part of their daily operations.
- **Firms are ethically obligated to protect this sensitive data, offering cybercriminals the opportunity for a quick payout**
- Law firms are also run by attorney who usually have little to no background and experience with cybersecurity matters

Copyright © 2021. Law & Forensics. Privileged & Confidential. Not for distribution or publication.

Who is attacking law firms?

Hackers/ Hacktivists

Aim to expose secrets (whistleblowers) by finding loopholes.

WikiLeaks

Criminals

Target the cash-rich and data-rich. Weapon of choice: Ransomware

KIA

Nations

Funded by nations/ governments. Aim to exfiltrate data, divert funds, and steal information.

Honda

Human Error

Vulnerabilities due to user errors and lack of adherence to security protocols.

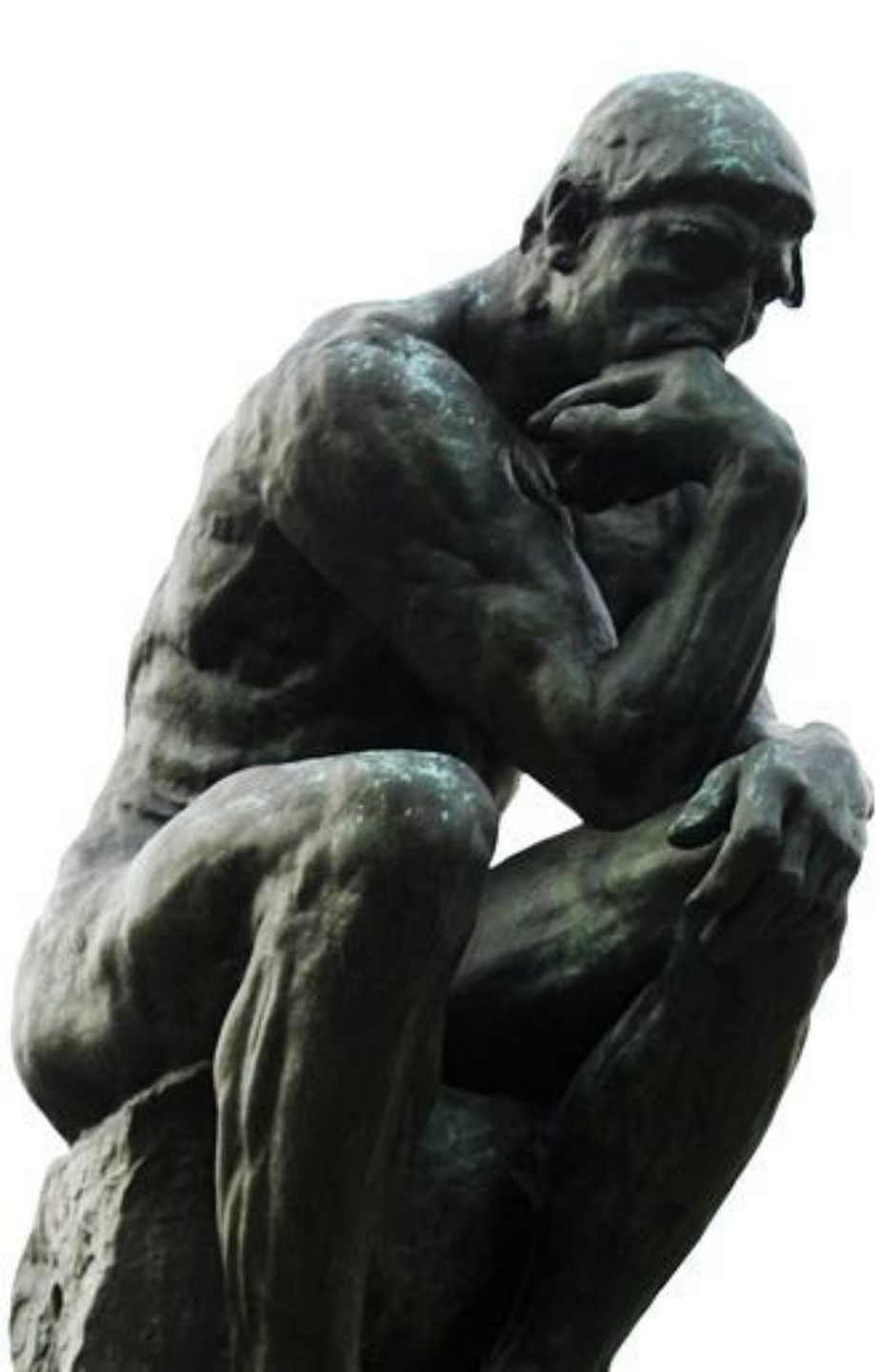
Tesla

Inside Agents

Disgruntled former employees, or criminals looking to get privileged access.

LAW & FORENSICS
A Global Legal Engineering Firm

Copyright © 2021. Law & Forensics. Privileged & Confidential. Not for distribution or publication.



Law firms work with large companies with confidential data that can be sold to other bad actors.

Social Engineering

- Law firm employees/partners accidentally provide attackers with information that can unlock data

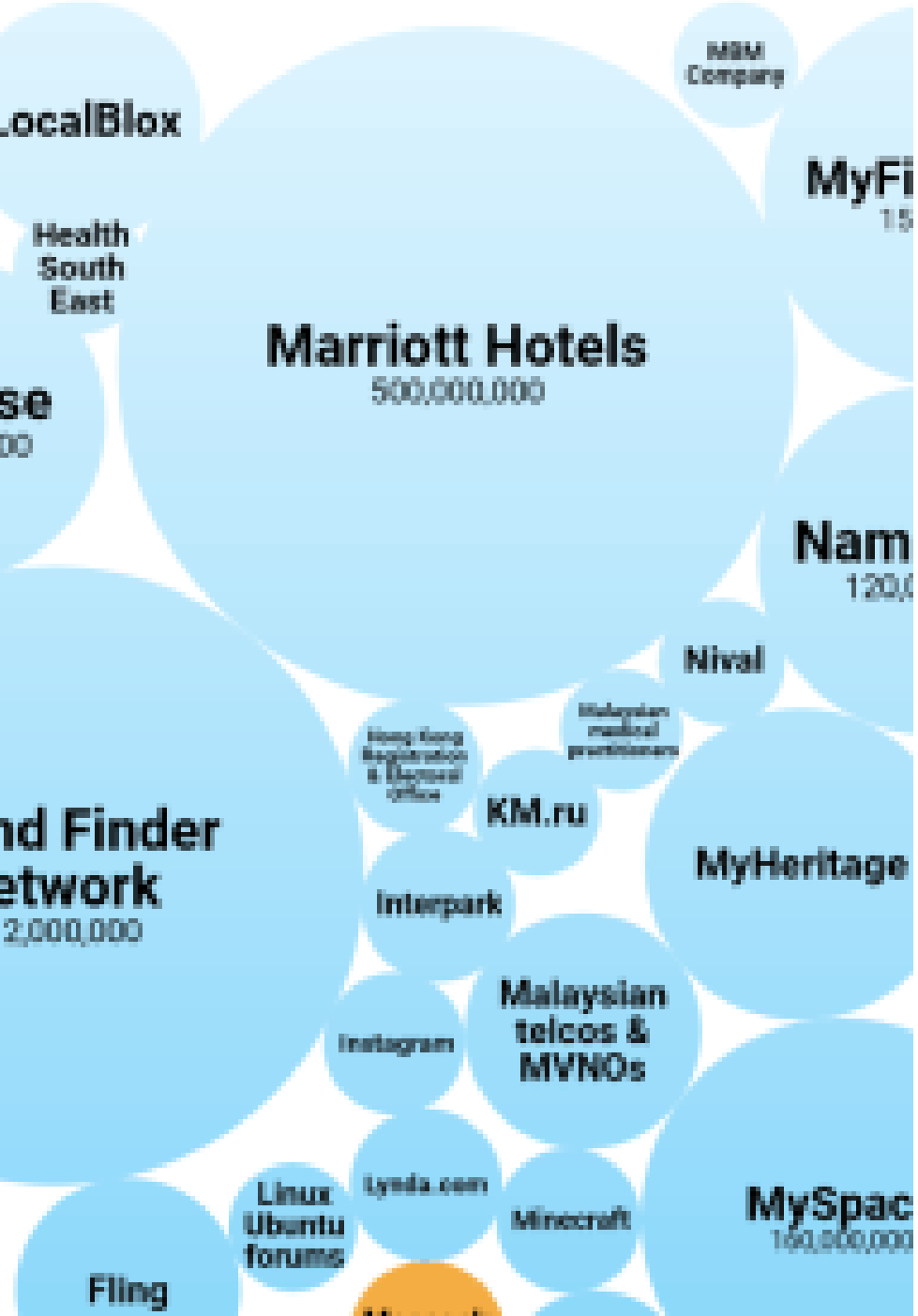
Phishing

- Trying to acquire username/passwords or get a user to click a link by posing as a trustworthy source
- Traditionally take place over email

Malware

- Spearfishing and put malicious code on a server
- Sends passwords, files, emails back to the attackers

Copyright © 2021. Law & Forensics. Privileged & Confidential. Not for distribution or publication.



Not All Data Security Incidents are Breaches/Hacks

- Cyberattacks against law firms have risen as a result of the pandemic and remote work.
- The security breach notification laws for most states only require businesses to report attacks that have exfiltrated data containing personally identifiable information
- For example, when the data is encrypted, it doesn't necessarily mean that an unauthorized person had obtained the information. However, the firm may have been hacked and systems made inaccessible and impaired your ability to operate remotely or in-person.

Copyright © 2021. Law & Forensics. Privileged & Confidential. Not for distribution or publication.

SolarWinds

and Other Notable Third Party Law Firm Hacks

SolarWinds Attack

- On December 13, 2020, FireEye announced the discovery of a highly sophisticated cyber intrusion that leveraged a commercial software application made by SolarWinds.
- It was determined that the advanced persistent threat (APT) actors infiltrated the supply chain of SolarWinds, inserting a backdoor into the product. As customers downloaded the Trojan Horse installation packages from SolarWinds, attackers could access the systems running the SolarWinds product(s).
- The United States government determined the attack posed a "grave risk to the Federal Government and state, local, tribal, and territorial governments as well as critical infrastructure entities and other private organizations."

Copyright © 2021. Law & Forensics. Privileged & Confidential. Not for distribution or publication.

SolarWinds Details (cont.)

SEC Response to Solar Winds	SolarWinds told the SEC that up to 18,000 of its customers installed updates that left them vulnerable to hackers.
	The US Securities and Exchange Commission is investigating companies who failed to disclose the effects of the SolarWinds hack.
SEC Current Actions	SEC is offering amnesty to companies that come forward and disclose the impact of the hack on their business.
	The SEC will pursue enforcement actions and heightened penalties to companies who have not properly disclosed the impact of the hack.

Copyright © 2021. Law & Forensics. Privileged & Confidential. Not for distribution or publication.

SolarWinds Details (cont.)

In a February congressional hearing, Microsoft president Brad Smith stated that more than 80% of the victims targeted were nongovernment organizations.

Victims: **Employee email accounts from 27 US Attorneys' offices**; parts of the Pentagon, the Department of Homeland Security, the State Department, the Department of Energy, the National Nuclear Security Administration, and the Treasury, Microsoft, Cisco, Intel, Deloitte, and others.

Copyright © 2021. Law & Forensics. Privileged & Confidential. Not for distribution or publication.

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

SolarWinds - Lessons

Check list for Third Party Risk Management is not effective

Active inventory of software assets is critical and prioritize software.

Revisit how your critical software manages the SDLC (SSDLC)

Copyright © 2021. Law & Forensics. Privileged & Confidential. Not for distribution or publication.

Seyfarth Shaw LLP & Fragomen, Del Rey, Bernsen & Loewy LLP

- Both BigLaw firms announced security incidents, involving a malware attack that risked clients' sensitive information
- In the Seyfarth case, the ransomware attack involved criminals freezing the victims out of the network and demanding payment to restore access. The firm reported it had restored all critical systems and that no client/firm data was accessed
- In the Fragomen data breach, an "unauthorized third party" gained access to a file with the employment eligibility data of Google staffers. This breach was most likely caused by credential compromise rather than malware

Copyright © 2021. Law & Forensics. Privileged & Confidential. Not for distribution or publication.

Microsoft Exchange Hack

- On March 2, Microsoft announced vulnerabilities in their Exchange Server mail and calendar software used by corporate and government data centers. However, the vulnerabilities had been in the code base for over ten years
- As a result of these vulnerabilities, Chinese hackers infiltrated, trying to gain information from defense contractors, schools, and other US entities.
- The **hack infected** about **60,000 global victims** with malware including **numerous law firms.**

Copyright © 2021. Law & Forensics. Privileged & Confidential. Not for distribution or publication.

Accellion

- **Accellion was slow to raise the alarm about the risks of their file transfer system, giving the hackers a "large time window for active exploitation."**
- Large companies including Kroger, Singtel, the Australian Securities and Investments Commission, and the University of Colorado were impacted by the breach.
- Goodwin Procter was alerted that their file transfer system was accessed by an unauthorized user, who gained access to stored data.
- Jones Day was also hit by a data breach resulting from Accellion hack, a hacker known as Clop posted files, including a confidential memo to a judge, claiming to be from the Jones Day breach.

Copyright © 2021. Law & Forensics. Privileged & Confidential. Not for distribution or publication.

Strategies

For managing your cyber risk

Sleep with One Eye Open

Even if you have secured your firm, the vulnerability might come from your third-party vendors.

- Vet your vendors for risks and track the news for potential vulnerabilities
- Use experienced technology companies have groups dedicated to third-party vetting and should be used and while this may increase costs in the short run, it will pay off in the long run
- Hire security consultants during the contract negotiation process and take advantage of services that can help them rate the risks of their potential vendors

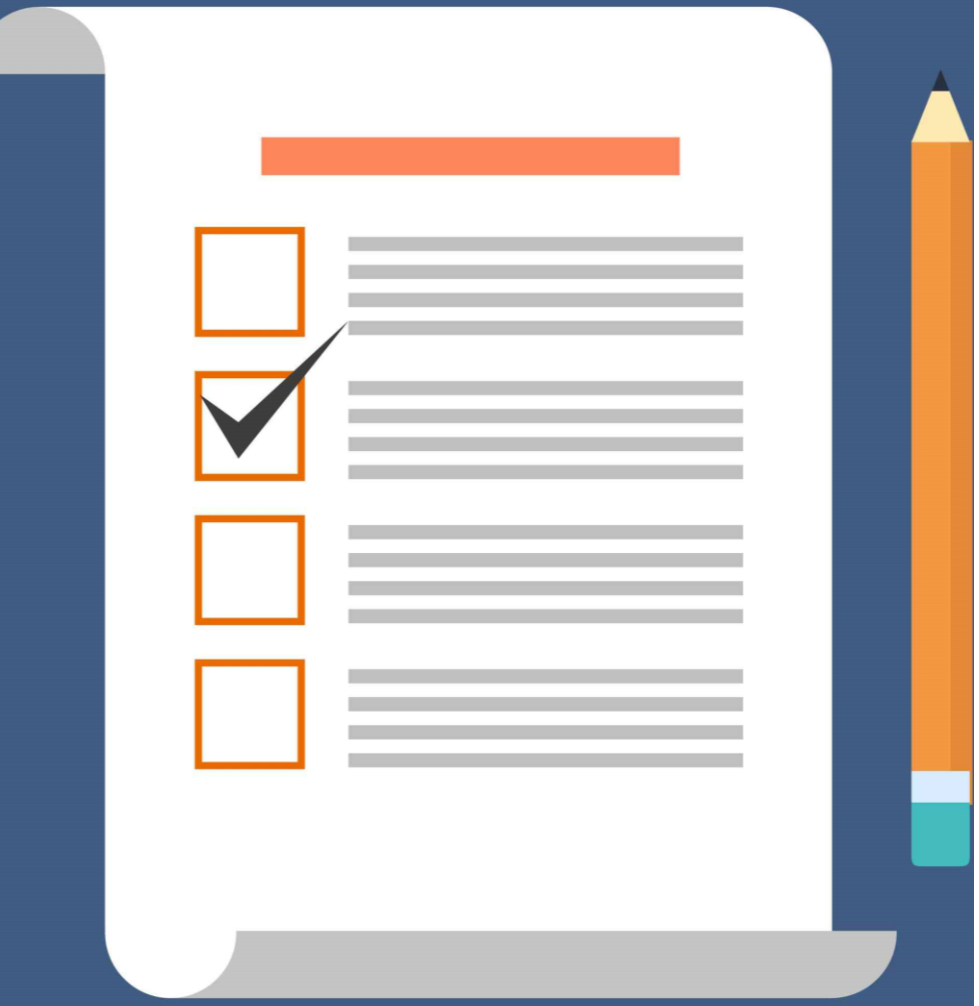
Copyright © 2021. Law & Forensics. Privileged & Confidential. Not for distribution or publication.

Defense-in-Depth

Design and deploy

- Defense-in-Depth (DiD), also known as the "castle approach," is a cybersecurity method of layering defensive mechanisms to protect valuable data and information.
- The layered approach strengthens the security of the system and covers different attack vectors
- Common security elements found in a DiD:
  - Network Security Controls
  - Antivirus Software
  - Analyzing Data Integrity
  - Behavioral Analysis

Copyright © 2021. Law & Forensics. Privileged & Confidential. Not for distribution or publication.



Incident Response Plan

Develop and Test

- Engage all key areas (business, legal, marketing, insurance, HR, IT).
- Develop a cross-functional incident response plan and team
- Retain outside technical, legal, and PR experts for the inevitable cyber incident and identify points of contact within law enforcement before a cyber-attack.
- **Test it!**

Copyright © 2021. Law & Forensics. Privileged & Confidential. Not for distribution or publication.

Cybersecurity Insurance

Evaluate and Purchase

- 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 IR plan
- Stay abreast of the market -- cyber insurance is still evolving, coverage and pricing are in progress
- Policies and available products must be continuously reviewed for gaps

Copyright © 2021. Law & Forensics. Privileged & Confidential. Not for distribution or publication.

Key Takeaway

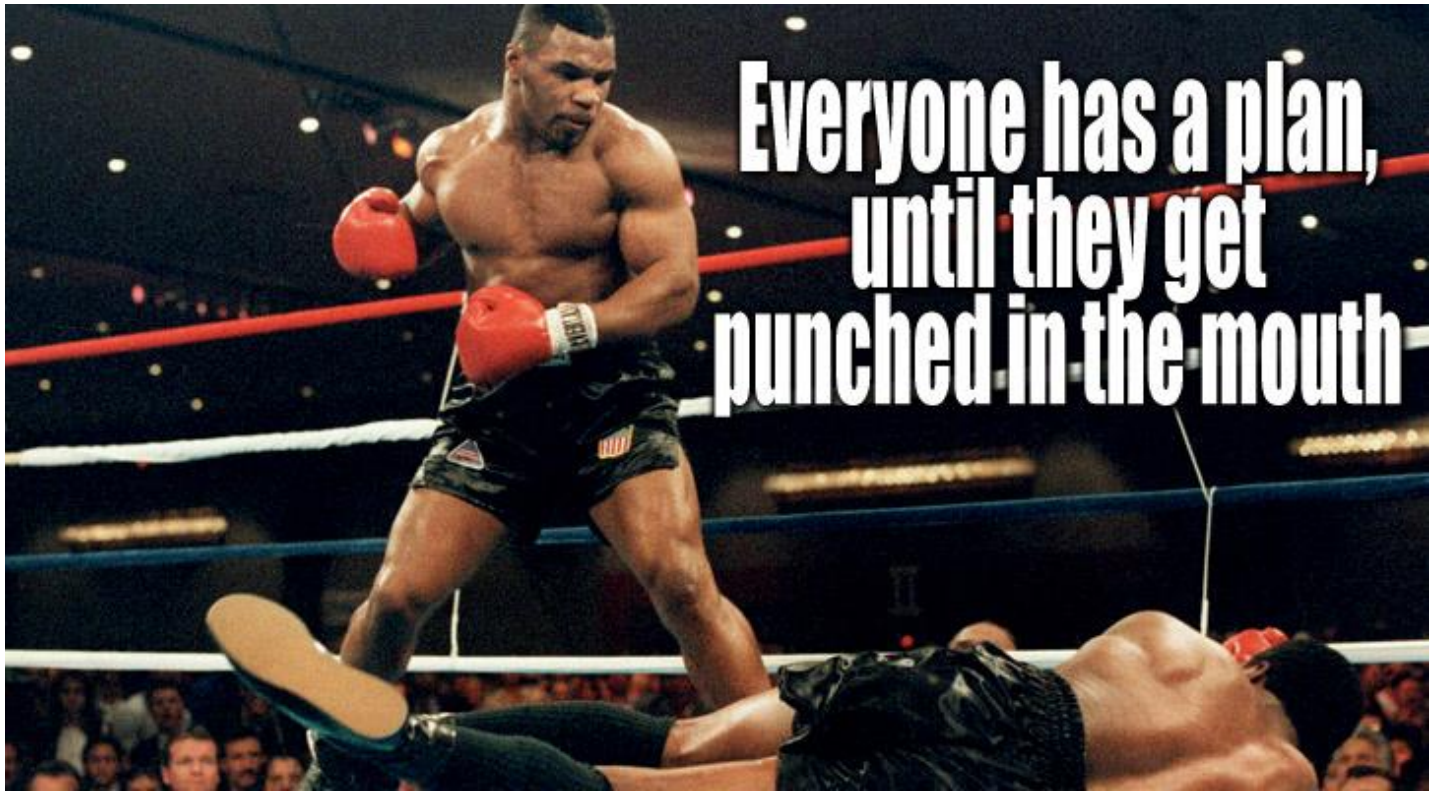
Devil is in the details

Copyright © 2021. Law & Forensics. Privileged & Confidential. Not for distribution or publication.

Be prepared

Copyright © 2021. Law & Forensics. Privileged & Confidential. Not for distribution or publication.

Establish and test an incident response plan



Copyright © 2021. Law & Forensics. Privileged & Confidential. Not for distribution or publication.

Define and test communication protocols.

Copyright © 2021. Law & Forensics. Privileged & Confidential. Not for distribution or publication.

Contact Us

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

David Cass
Email: davidcassciso@gmail.com
URL: https://www.newyorkfed.org/

Daniel B. Garrie
Co-founder of Law & Forensics
Neutral with JAMS

Contact:
E: daniel@lawandforensics.com
URL: https://www.lawandforensics.com

LAW & FORENSICS
A Global Legal Engineering Firm

Daniel Garrie, Esq. is the Co-Founder of Law & Forensics LLC, where he heads the Computer Forensics and Cyber Security teams. Daniel has been a dominant voice in the computer forensic and cybersecurity space for the past 20 years as an attorney and technologist.

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 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 cyber and forensic teams in some of the most visible and sensitive cyber incidents in the United States. He and his team have done work for three sitting U.S Presidents and several U.S. Attorney Generals, two of the top five banks in the globe, dozens of the largest private and public companies in the world, and in nearly every industry. Daniel and his team have been involved in thousands of investigations and disputes all over the globe. In addition, Daniel has been awarded several patents, which technology is used in an advanced cybersecurity and forensic platform he built with his team (Forensic Scan) that is currently used in the industry.

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

David Cass
Federal Reserve Bank of New York – Vice President, Cyber & IT Risk
Contact:
E: davidcassciso@gmail.com
URL: https://www.newyorkfed.org/

David is the Vice President for Cyber & IT Risk for the Federal Reserve Bank of New York. Prior to this role, David served as the Chief Information Security Officer for IBM. He had global responsibility for all aspects of security practices, processes, and policies across the IBM Cloud SaaS business unit.

Previously David served as the SVP & Chief Information Security Officer for Elsevier. Where he lead an organization of experienced legal, risk and security professionals that provided data protection, privacy, security, and risk management guidance on a global basis for Elsevier.

David has extensive experience in IT security, risk assessment, risk management, business continuity and disaster recovery, developing security policies and procedures. He has played a key role in leading and building corporate risk & governance and information security organizations in the financial sector. As the Senior Director of Information Security Risk and Governance for Freddie Mac, David rebuilt the risk and governance function and developed a team to provide risk assessments, methodologies, tools, services, and training to improve the organization's capabilities and maturity. Prior to that he was Vice President of Risk Management for JPMorgan Chase, and was responsible for providing an accurate assessment of the current risk management state, contributing to the future direction of risk management, continuity and disaster recovery capabilities for the organization.

David has a MSE from the University of Pennsylvania, and a MBA from MIT. He is also a frequent speaker at high profile industry conferences, and serves on the Board of Directors for PixarBio Corporation.

the 20TH ANNUAL LAW FIRM COO AND CFO FORUM

Breakout 4:
Stir of Echoes: Law Firm Lessons from the SolarWinds Hack

David Cass
Vice President – Cyber & IT Risk,
Federal Reserve Bank of New York

Daniel B. Garrie, Esq.
Co-Founder,
Law & Forensics LLC