A ROUNDTABLE DISCUSSION

CYBERSECURITY

THE STRATEGIES COMPANIES NEED TO KEEP THEIR DATA SAFE

As cyberattacks become more sophisticated and harder to trace, it's critical for companies to be ready for them. Three experts from Chicago's cybersecurity scene discuss trends in the cybersecurity arena and how companies can better prepare for cyberattacks.

JOEL B. BRUCKMAN
Partner
Freeborn & Peters LLP
jbruckman@freeborn.com
312-360-6461

MATTHEW P. CONNELLY
Founder/Principal
Rock Fusco & Connelly LLC
mpc@rfclaw.com
312-494-1000

RYAN T. SULKIN
Partner
Benesch
rsulkin@beneschlaw.com
312-624-6398

What are cyber criminals trying to achieve and how have cyberattacks changed in recent years?

Joel Bruckman: Financial gain remains the focus of the overwhelming majority of cybersecurity incidents. Attack vectors have evolved in functionality to integrate the exfiltration of data as a means to leverage the financial reward associated with cybersecurity attacks, which includes demands for ransom. Furthermore, nefarious actors continue to use "payloads" which focus on the secondary distribution of their malware to exponentially grow the reach of their attack campaign. For example, instead of only breaching a single email account and accessing or exfiltrating data therein, malicious "payloads" are being designed to autonomously launch successive phishing campaigns using the contacts stored within compromised email accounts, thus growing the web of potential victims and inflating the potential financial gain of an attack.

Ryan Sulkin: Malicious actors are seeking to achieve two primary objectives, sometimes at the same time. The first objective is theft of personal data or other intellectual property that can be quickly monetized via the dark web or other networks and/or held for ransom. The second objective is operational disruption. For example, shutting down the ability of a company to conduct business because its computerized systems have been rendered inoperable.

> "FOR BUSINESSES WITHOUT A PROPER BACKUP OF DATA AND WITHOUT CYBER LIABILITY INSURANCE, A RANSOMWARE ATTACK COULD BE FATAL TO THEIR EXISTENCE."
>
> — JOEL BRUCKMAN, FREEBORN & PETERS

Matthew Connelly: As we all know, cybercriminals seek monetary gain by accessing personal information and transferring money through deception or ransomware. However, an equal, less discussed motivating factor is competition. The bad guys seek advantage over rival organizations through cyberattacks. Social attacks use emails, texts and calls to trick users into clicking on links. Email is predominantly used to deliver ransomware, crimeware, malware, viruses and worms. Web application attacks are code and vulnerability exploits, overcoming authentication using stolen credentials. This allows for SQL injections– code injection techniques that can result in database modification or administrative operations control. The worst part is, detecting threats has become increasingly difficult, an evolution that allows cybercriminals to remain undetected, obtaining as much data as possible.

Are certain industries or types of intellectual property more likely to be targeted for cyberattacks?

Sulkin: Industries that are considered critical infrastructure for the country (e.g., power, manufacturing, shipping and logistics) are likely to be targets because of the disruption that an attack would cause. In addition, industries that trade in highly-sensitive or highly-regulated data, for example, financial institutions or hospitals/health care, are more likely to be targeted, due to the sensitivity and value of the data involved in the operation of their business.

Connelly: Trade secrets are a likely target for cyberattacks as they are sensitive intellectual property consisting of exclusive information highly confidential in nature. We have seen evidence of this type of targeted behavior through notable cyberattacks such as the breach of the SolarWinds Orion software which sought government agency and private company information, specifically corporate trade secrets.

How has the increase in ransomware demands affected businesses?

Bruckman: The increase in ransomware demands has made cyber liability insurance even more of a necessity than before. For businesses without a proper backup of data and without cyber liability insurance, a ransomware attack could be fatal to their existence. Moreover, the increase in ransomware demands has further hardened the cyber insurance market resulting in significant increases in premiums. Insurers are also implementing proactive measures to test potential insured's vulnerabilities by including security assessments as part of their underwriting process, such as penetration or "pen" testing.

Connelly: In talking with my colleague Brittany Haracz, we see that the biggest change in ransomware has been the evolution of threats involving demands of a few hundred dollars to the emergence of ransomware more akin with business operations. With this evolution comes an increase in demand, now upwards of millions of dollars which has a major impact on affected industries. Because of this, the financial damage continues

CYBERSECURITY

THE STRATEGIES COMPANIES NEED TO KEEP THEIR DATA SAFE

to prove an issue that businesses affected by ransomware demands face. Another impact of ransomware attacks is significant damage to business reputation. Finally, the threat of leaked data due to ransomware demands can jeopardize sensitive company data and result in increased likelihood of cyberattacks in the future, meaning that once an attack takes place, there may be greater likelihood of another attack.

Sulkin: Businesses are increasingly focused on ransomware prevention and the purchase of cybersecurity insurance to cover cost and expense in the event of a ransomware attack. In addition, businesses are focused on their business continuity and disaster recovery strategies, including frequent testing of those strategies.

What can organizations do to ensure they are prepared for a data security incident?

Bruckman: The best defense for proactively defending against ransomware, or any other cyber threat, is providing proper training to employees and oversight to ensure compliance with policies and procedures which provide administrative safeguards. That said, ransomware attacks are significantly thwarted where the encrypted data is backed-up. The off-site backup of data is critical in shifting the leverage back toward the victim of a ransomware attack because it lessens the need for the decryption of data which can otherwise be restored through backups. Partitioning networks across an enterprise to keep the most sensitive data segregated from other users can also be an effective means to thwart the propagation of ransomware across a company's network.

Connelly: To mitigate the risks to IP, companies should consider enacting policies that monitor and audit access to sensitive information in order to identify a potential cyber-attack. Additionally, it may be worth contracting with a vendor management program that specializes in data security. Constant vigilance as to who has access to secure information and how this information is secured remains an integral mitigation strategy. Also, they should frequently change passwords and establish multi-factor verification, in addition to keeping employees aware of current cybercriminal activity.

Sulkin: Best practices for avoiding ransomware threats include use of industry standard security measures to prevent intrusion (multi-factor authentication and rigorous endpoint monitoring), prompt vulnerability remediation and rigorous employee training to help minimize the likelihood of a successful phishing or social-engineering based attack. In addition, having data and applications backed-up in alternate, offline locations that can be readily restored to production and will not be impacted by a ransomware attack is critical. With this in place, it may not be necessary to pay the ransom in the first place.

What are some of the must-haves of a good incident-response plan?

Sulkin: It's critical to have a documented incident response plan and to test that incident-response plan regularly, for example, through tabletop exercises. The incident-response plan serves as a step-by-step guide for how a business will address a data security incident, including who will be involved, how the investigation of the incident will be managed, which key decisions need to be made, and how information will flow between key stakeholders at a company. A sound incident-response plan should also consider the unique business practices of the company. For example, certain technologies may require special attention due to operational need or to contain particularly sensitive data. In addition, the incident-response plan must take into account management of internal and external communications such as PR and communications to employees.

> "DETECTING THREATS HAS BECOME INCREASINGLY DIFFICULT, AN EVOLUTION THAT ALLOWS CYBERCRIMINALS TO REMAIN UNDETECTED, OBTAINING AS MUCH DATA AS POSSIBLE."
>
> — MATTHEW CONNELLY, ROCK FUSCO & CONNELLY

Bruckman: A good incident-response plan should include incident-response points of contact (legal, IT, insurance, C-suite, vendors); the location and storage of sensitive data (who, what, where), known applicable regulatory guidelines or statutory laws which prescribe short notification deadlines (CCPA, GDPR) and a strategic process to mitigate damage or the propagation of a cybersecurity incident (network mapping, identification of backups, other computer systems susceptible to infection on common networks).

How can companies stay on top of evolving and new cybersecurity threats?

Connelly: The need to stay "in the know" is imperative. Since risk assessment is paramount in determining the likelihood of a cybersecurity attack, there are several practices based on individualized company evaluations that can help predict potential threats. For example, the FCC provides a cybersecurity planning tool that assists companies in implementing strategies based on specific business needs and activity. Additionally, the Department of Homeland Security offers a self-assessment that can be informative in evaluating a company's operational resilience and effectiveness of cybersecurity procedures. Beyond security evaluations, companies should make use of antivirus software, specifically designed to detect constantly evolving cybersecurity threats and ensure that company devices are equipped with this software and updated frequently. Of course, attending and requiring that employees participate in training surrounding cybersecurity is essential to staying on top of cybersecurity threats.

Bruckman: Companies should go to their data privacy counsel, managed services providers, and cybersecurity IT firms, which are all good sources of information on current cybersecurity trends, campaigns and issues. Google alerts, National Law Review and various online publications are also helpful and offer a wealth of information. Cyber insurance carriers may also offer resources.

Sulkin: Information comes from multiple sources. Third-party providers of monitoring, detection, and threat hunting services provide tremendous insight regarding known attacks. In addition, software companies regularly provide updates and patches in order to address emerging threats or known weaknesses. Timely deployment of these updates and patches is of critical importance. Finally, government and law enforcement agencies release information regarding threats, and this information should be tracked as well.

What are some of the biggest lessons that organizations can learn from data security incidents?

Sulkin: Data security incidents often help organizations improve their own security measures, as much will be learned about exploited weaknesses during the investigation of the incident. In addition, organizations after a data-security incident often review their larger approach to data governance, to see, for example, if the amount of data retained on a go-forward basis can be minimized or isolated to highly secured zones. Finally, after a phishing attack or other social-engineering based attack, a renewed focus is often put on employee training, to help team members better identify the signs of an attack in advance.

Connelly: First, policies and procedures should be properly implemented and well-documented, taking a risk-based approach when it comes to security. Additionally, there should be strong internal oversight ensuring that consumer information such as personally identifiable information is protected through layered security controls including but not limited to intrusion protection and detection, multi-factor authentication, password complexity and routine vulnerability assessment. The importance of employee training is a key lesson learned from cyber-security incidents.

Bruckman: Cyber liability insurance is a must. Inadequate document retention policies can cost hundreds of thousands of dollars in the event of a business email compromise. If employees are not trained to ensure compliance with policies and procedures, even the best technological safeguards can still be extremely vulnerable to a cyber attack. Cybersecurity incidents don't end once the threat has been neutralized, because legal notification obligations may be triggered which may include reporting to governmental agencies and affected individuals who may need to be provided with identity protection products and services. Government investigators will most likely inquire about pre-incident data protections.

How can companies best prepare to defend themselves in a litigation if they should have a future data breach?

Sulkin: State laws are increasingly requiring compliance with data security requirements and, in some cases, directly opening the door to claims from plaintiffs who, due to the availability of statutory damages under these regimes, will not need to overcome historical hurdles proving actual damages. Companies must rigorously maintain documentation and other "proof" of the reasonableness of their security programs in order to be best positioned to defend themselves in court. It is incredibly difficult to create proof of a reasonable security program after the fact, meaning once a breach has occurred and the litigation has commenced.

> "COMPANIES MUST RIGOROUSLY MAINTAIN DOCUMENTATION AND OTHER PROOF OF THE REASONABLENESS OF THEIR SECURITY PROGRAMS IN ORDER TO BE BEST POSITIONED TO DEFEND THEMSELVES IN COURT."
>
> — RYAN SULKIN, BENESCH

Bruckman: When defending against claims in litigation related to a data-security incident, diligence in the protection of information prior to the attack, an appropriate response to the attack, and timely notification to affected individuals (if necessary) needs to be demonstrated. One also needs to be aware of legal privileges which may attach to an investigation of a data security incident and that proper steps are taken to ensure such privilege attaches immediately through the engagement of legal counsel.

How do you see the framework set forth in the Strengthening American Cybersecurity Act (SACA) affecting the preparedness and incident response planning of critical infrastructure industries?

Bruckman: Because the executive order allows for the construction of the actual law to take place over the next two to three years, time will tell as to what SACA will look like. There will be very short notification timelines for critical infrastructure to make an initial notification of a cybersecurity incident, which includes providing notice to the Cybersecurity and Infrastructure Agency (CISA) within 72 hours (24 hours in cases of ransomware), providing a description of the incident and vulnerabilities exploited, advising of what defenses were in place, the nature of the information that may have been compromised and more. Critical infrastructure organizations will need to have a proper incident-response plan at the time of an incident, as well as a robust set of safeguards to protect data. SACA will bring some semblance of continuity in terms of notification obligations at the federal level, in addition to state and regulator obligations. SACA will also likely lead to a greater number of enforcement actions for non-compliance in due course.

Connelly: A key attribute of SACA is the new timeline requirements for reporting data breaches. Owners and operators of critical infrastructure industries must report cyber incidents to CISA, an agency of the U.S. Department of Homeland Security, within 72 hours. Additionally, ransomware payments to cybercriminals must be reported by affected critical infrastructure operators within 24 hours of the activity. These two integral timelines impose specific timeframes for reporting a breach. Be aware of the scope of these timelines in preparation for the possibility of reporting a cyberattack and consider developing a response policy to adhere with the timelines required by law. Based on the framework of the act, companies should assess whether their business will be covered and should develop procedures for reporting cyber crimes in a timely manner. Above all else, companies must take necessary precautions to protect themselves from breaches in cybersecurity to avoid becoming victims of cybercrime.

ABOUT THE PANELISTS

JOEL BRUCKMAN is a partner in Freeborn & Peters' litigation practice group and insurance/reinsurance and emerging industries teams. Bruckman focuses on complex commercial litigation, and he dedicates a significant portion of his practice to advising clients on data privacy and cybersecurity issues, including proactive preparedness and reactive incident response. As a former financial crimes prosecutor, Bruckman has extensive experience in white-collar criminal investigations and post-indictment matters. He is a former Cook County State's Attorney and former member of the FBI's Cyber Crimes Task Force.

Freeborn

MATTHEW CONNELLY is principal and co-founder at full-service law firm, Rock Fusco & Connelly, LLC. Connelly practices in a myriad of areas including cyber security law; commercial and securities litigation; insurance coverage litigation; and general tort and product liability law. He has tried numerous jury and bench trials in all areas of litigation, and has co-authored and presented numerous seminar materials and articles on various topics such as cyber law. Connelly is a former member of the Privacy and Information Security Law Section Council of the Illinois State Bar Association.

R·F·C
ROCK FUSCO & CONNELLY, LLC
ATTORNEYS AT LAW

RYAN SULKIN is a partner with Benesch and leads the firm's Data Protection Group. He regularly advises clients regarding complex technology transactions, including SaaS, software development, professional services and outsourcing arrangements. He also provides risk-based and actionable legal counsel on data privacy and cybersecurity matters across a wide range of industries, including financial services, payments, health care, higher education, retail, hospitality and technology. Sulkin's experience includes designing security and data governance programs to protect and properly manage trade secrets.

Benesch