ROUNDTABLE DISCUSSION CYBERSECURITY

SPONSORED CONTENT

How to keep your organization or company safe from increasingly sophisticated security breaches

Cyberattacks are omnipresent in the digital world as data flows through systems and networks at breakneck speed. One accidental click on a hyperlink from what appears to be a legitimate email address can lead to a serious data breach and costly consequences for a company or organization. Attacks are becoming more advanced and intentional, leaving business leaders struggling to figure out how to stay ahead of and anticipate new threats. Crain Content Studio — Cleveland turns to four cybersecurity experts who discuss some of the most common concerns, and what leaders can do to be sure their data, operations and people are protected.

THE EXPERTS

JOE COMPTON
Principal
Skoda Minotti Risk Advisory Services

SKODA MINOTTI
RISK ADVISORY SERVICES
Delivering on the Promise.

Joe Compton is a principal in Skoda Minotti’s Risk Advisory Services practice. With more than 30 years of IT and business management experience, he has spent the past 20 years focused on compliance and technology security management for regulated industries, including banking, health care and technology companies. As a certified information systems auditor (CISSP), qualified security assessor (QSA), core impact certified professional (CICP) and certified information security professional (CISA), Joe’s consulting practice is focused in four main areas: IT security audit and penetration testing; IT security program development; risk assessment facilitation; and business continuity planning. He is a 1989 graduate of John Carroll University with a bachelor of arts degree in English and history, and he earned in 2012 a certificate in executive management from the University of Notre Dame Mendoza College of Business. A lifelong learner, he is a graduate of Leadership Cleveland (2014) and the Mandel Leadership Program (2014) at the Cleveland Jewish Federation. Joe served on the board of Lake Catholic High School and chaired the technology committee for the Jewish Federation of Cleveland. Joe is also a board member on various Cleveland technology startups. He lives in Lakewood.

STEPHANIE J. DINGMAN
Senior Vice President
and Cyber Team Leader
Aon Risk Solutions

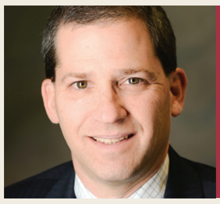
AON
Empower Results®

Stephanie Dingman is a team leader for Aon, a global professional services firm. Stephanie manages a team of brokers and helps clients across the country address Cyber and Errors & Omissions exposures. Her areas of expertise include network security and privacy liability; technology errors and omissions; professional liability; and media liability. Stephanie advises clients on all aspects of cyber resilience, utilizing market leading solutions and proprietary data and analytics. She holds the following designations: chartered property casualty underwriter, associate in risk management and certified insurance counselor. Stephanie earned a bachelor’s degree in business administration with an emphasis on actuarial science and risk management and insurance from University of Wisconsin, and an MBA in finance from University of Minnesota.

BOB ECKMAN
Chief Information Security Officer
MCPc

MCPc

Bob Eckman is chief information security officer at MCPc Inc. in Cleveland. He also is an adjunct professor at Kent State University and at Cleveland State University’s Cleveland-Marshall College of Law, specializing in cybersecurity and digital systems security. He also serves as leading contributor and interim executive director of the Cleveland State University’s Center for Cybersecurity and Privacy Protection. Bob’s career background includes serving as cybersecurity program manager, during which he implemented the NEI 08-09 Cyber Security Program for Nuclear Power Generating facilities in response to 10.CFR 73-54. As part of these responsibilities, Bob served as chairman of the Nuclear Information Technology Strategic Leadership and a member of the Nuclear Energy Institute’s Cyber Security Task Force in Washington, D.C. In addition to cybersecurity, Bob is an experienced technologist and project specialist, having earned both his project management professional (PMP) and certified information systems security professional (CISSP) certificates along with his master’s degree.



MIKE STOVSKY
Partner and Chair of the Innovations,
Information Technology & Intellectual
Property Practice Group
Benesch

Benesch
Attorneys at Law

Mike Stovsky is a partner and chair of one of Benesch’s core practice groups, Innovations, Information Technology & Intellectual Property (3iP). Mike has led the growth of the 3iP group from nine to 27 professionals nationally. He also has spearheaded the transformation of the group to include comprehensive technology transactions and global data security and privacy. Mike helps companies handle deals and matters in the following areas: intellectual property, information technology, technology transactions, technology procurement, intellectual property transactions, licensing, systems implementations, technology transfer, intellectual property counseling, intellectual property commercialization and monetization, due diligence, life sciences, privacy, data security, advanced manufacturing, Internet, ecommerce, corporate, securities, venture capital and private equity. Mike is CIPP/US certified. He earned his undergraduate degree from Northwestern University and his law degree from the University of Pennsylvania. He is listed in The Best Lawyers in America, Information Technology Law (Woodward/White, 2007- present).

CRAIN CONTENT STUDIO
Cleveland

Q&A

What are the biggest concerns in terms of day-to-day business operations from a cybersecurity perspective?

MIKE STOVSKY: The biggest concerns today center around the potential impact of a cybersecurity incident on the business operations of a company, as well as the potential liability risks to the company from a cybersecurity incident. These risks include financial loss, reputational harm, having company data or systems held for ransom, governmental fines and penalties, private lawsuits and class action litigation.

BOB ECKMAN: The greatest challenge in our industry is knowing the unknowns. We should strive to go where the adversary is going to go next, and that's where we aren't looking. Verizon's Data Breach Investigations Report has identified the "Detection Deficit" is ever growing, that is: The time it takes from the point of compromise vs. the time it takes for us to detect (and even respond) to these breaches is not trending in our favor.

I'd like to say that new tools are the panacea to solve this issue, and although a great asset that's getting better, tools are simply not enough. Companies must get serious about how they are approaching cybersecurity from the top down. A chief information security officer, or CISO, in the boardroom who can effectively translate cyber risk into the language of business is a good start.

Tactical cyber leadership on the ground who can drive out comprehensive cyber programs that seek to integrate the operational (monitoring, threat hunting, detecting breaches, physical processes); the management (policies and procedures, training, awareness); and the technical (cybersecurity tools) is equally as important. Steps to prevent attacks should be linked directly to closing the attack surface to the organization and a portfolio management process that allows the cyber team to shift and focus on new, unknown, areas quickly.

What are the latest events impacting a company's cybersecurity risk profile?

MIKE STOVSKY: These include whether the company has established a chief cybersecurity officer with authority for technical and legal compliance; whether the company does business across international boundaries (and is subject to multiple, often conflicting, laws, rules and regulations); and whether cybersecurity risk has been elevated to the C-level and the board level in the company in terms of its importance and prominence as a business imperative.

JOE COMPTON: If you read the marketing, one would believe it is ransomware, but the biggest thing affecting a company's cybersecurity risk profile is the data they collect and how and where they choose to process that information. Most regulated businesses have a requirement to develop a vendor management program to understand vendor security profiles and financial health, and map what sensitive data they process or touch. All businesses should get serious about making this process more than a check-the-box exercise.

To reduce the risk, businesses need to have a better understanding regarding the controls they are supposed to have implemented when using a third party, and test those internal controls on a regular basis. There are also some that take unnecessary risks by processing data themselves because they don't "trust the cloud."

In many cases, if implemented properly, cloud services provided by Microsoft, Amazon and Google can be significantly more secure than hosting in a private data center where the business' IT group is responsible for all the security. It is tough for any company to match the security firepower found at these organizations. It is not perfect, but it is better than most organizations can hope to provide with a small IT staff.

> *Cyber projects should always help to improve the process or quality of an organization. . . As part of any good risk assessment, the question that needs to be asked: what is the impact if we don't fund the initiative?"*
>
> — **JOE COMPTON,** *Principal,* Skoda Minotti Risk Advisory Services

What are basic things a company can do to reduce the likelihood of an IT security incident?

STEPHANIE DINGMAN: Risk-resilient companies have shifted their approach to cybersecurity and the way they act — from reactive to interventionist to proactive and preventive. Among these actions:

■ **Create effective cybersecurity board governance and accountability.** Although there are still limited resources, such as a standard methodology or guidelines to help them navigate the issue, boards are increasingly adding cybersecurity to their agendas.

■ **Prioritize assets for cyber protection.** Companies must systematically evaluate assets and prioritize them for varying levels of cyber protection based on risk.

■ **Assess third-party relationships.** It's important to understand the security posture of every third party, vendor and customer.

■ **Formulate rigorous incident response plans.** Organizations must design, implement and test plans to minimize and mitigate the damage when a breach inevitably occurs.

■ **Invest in employee awareness and education.** Because even when a company arms itself to the teeth with cybersecurity measures, it can take one person opening a corrupt attachment to put the whole company in jeopardy.

■ **Incorporate cyber governance into the M&A due diligence process early, particularly in higher risk or heavily regulated industries.** Acquiring companies should get the CISOs around the table and conduct cyber due diligence earlier in the process, alongside financial and FCPA due diligence.

JOE COMPTON: If your organization is new to IT security, the easiest place to start is to go to www.pcisecuritystandards.org/document_library and download the prioritized approach tool for implementing a Payment Card Industry Data Security Standard (PCI DSS) and implement it. Look, this isn't going to guarantee your organization's immunity from all attacks, but the standard is easy to follow, and prescriptive (it tells you what you have to do to meet the control objectives). It is a great place to start.

MIKE STOVSKY: Establish a comprehensive set of policies and procedures for cybersecurity protection that are implemented on an enterprise-wide basis. Ensure that all subcontractors with which the company does business comply in full with the company's policies and procedures. Have adequate safeguards in place for their own systems.

A company should appoint a qualified chief privacy officer and ensure that the company's board of directors includes qualified members who understand cybersecurity risk and elevate the prominence of cybersecurity to the C-suite. They should involve outside counsel and outside cybersecurity consultants in the company's planning, procurement, outsourcing and compliance efforts.

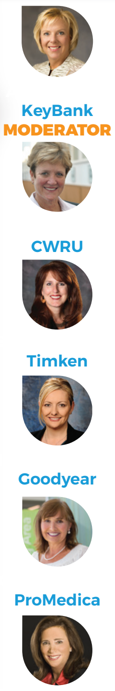
Additionally, an organization should enlist the services of a qualified managed services provider to provide comprehensive network monitoring, vulnerability assessment and threat mitigation services.

Does cybersecurity compliance equal security?

MIKE STOVSKY: No, there is a difference

CONTINUED ON NEXT PAGE

> *Firms value cyber policies because they provide support and expertise as insurers work with their clients to assess and mitigate cyber risk."*
>
> — **STEPHANIE J. DINGMAN,** *Senior Vice President and Cyber Team Leader,* Aon Risk Solutions



CONTINUED FROM PREVIOUS PAGE

between legal compliance and technical compliance. Both work hand in hand, but neither is exclusive. Both are necessary to overall compliance efforts.

JOE COMPTON: Look, Target was PCI compliant, and there was a data breach. A compliance audit just verifies controls are implemented and functioning. Controls are developed to prevent known security issues with systems from being exploited. The uphill battle we face as security professionals is, "How do you protect a system or network from the vulnerability that you don't see yet?"

Security is a process: risk assessment, control implementation, control testing, remediation and risk assessment. It should be a Möbius strip — a continuous loop that never ends.

What should any company focus on in the near-, mid- and long-term in terms of cybersecurity compliance?

MIKE STOVSKY: The latest advances in cybersecurity threat assessment, monitoring and mitigation.

JOE COMPTON: **Near-term:** Make sure your organization's network diagram is up to date, and your data classifications are up to date. An updated data flow diagram is helpful. Remember that data has three states: in use, in storage and in motion. Also, is your data encrypted, and how good are your originations backups? Conduct an IT risk assessment, and conduct IT security awareness training for your personnel.

Mid-term: Implement missing controls from risk assessment; conduct vulnerability assessments and patching; enhance log server capabilities and review items logged; and implement and test an IPS system.

Long-term: Develop an incident response plan and test it.

Who is responsible for managing cyber risk at an organization, and how often should they be communicating ongoing concerns, projects, etc. with leadership and employees?

MIKE STOVSKY: The chief privacy officer, the general counsel (or chief legal officer), the chief human resources officer and the board of directors.

STEPHANIE DINGMAN: There is a need to start shifting the approach and manage cyber as an enterprise-wide risk. It is important to work collaboratively across various stakeholders to implement good governance and frameworks, execute a resilience strategy and create a culture of risk, compliance and cybersecurity. Here's why:

■ **CEOs** want to satisfy their fiduciary duty, understand any legal, regulatory and financial implications of the risk and ensure a return on investment.

■ **CISOs** think about security improvements, transformation and remediation.

■ **Risk managers, CFOs and treasury** focus on the risk, align strategy and buy-in from stakeholders on necessary investments including the transfer of cyber risk exposure through cyber insurance.

■ **HR** stresses protecting HR sensitive data, counterproductive behavior, training to mitigate cyber threats and creating a culture of awareness.

■ **Legal and compliance** focuses on privacy data and managing the various regulatory position.

■ **CROs** want to mitigate increased cyber risk that mass connectivity means for operations and supply chains.

How can we get cyber projects approved when companies are focused on return on investment?

JOE COMPTON: Cyber projects should always help to improve the process or quality of an organization. There should be an operational reason to implement those security controls — improve availability of systems, improve the processing integrity of a system and improve the security of a system. Management should also take time to re-engineer inefficient processes when implementing security controls. As part of any good risk assessment, the question that needs to be asked: what is the impact if we don't fund the initiative?

STEPHANIE DINGMAN: While it's difficult to quantify the ROI on a particular cyber project, we do know that there is a cost to not focusing on it. In the months since Petya, five public companies have had to adjust their financial statement disclosures.

> *"A company should appoint a qualified chief privacy officer and ensure that the company's board of directors includes qualified members who understand cybersecurity risk and elevate the prominence of cybersecurity to the C-suite."*
>
> — **MIKE STOVSKY,** *Partner and Chair of the Innovations, Information Technology & Intellectual Property Practice Group,* Benesch

This is just a fraction of the impacted companies (as only public companies are required to publicly disclose) but certainly confirms the need for continued focus on IT security.

What are cyber insurance policies designed to cover?

BOB ECKMAN: It has been our experience that cybersecurity insurance policies are meant to cover damages relative to the actual breach. These may include physical asset impacts, such as having to replace equipment, and/or relative data impacts. For instance, should sensitive information be made available to unauthorized individuals, it could result in damages, some form of credit or identity protection, and/or brand defense, legal defenses, etc.

What is yet to be understood in total is how insurers are handling resulting investigations and fines from organizations like the Office of Civil Rights (HIPAA), which has levied an impressive number of fines over the past two years with both the frequency and penalty growing as of late.

The question of whether cyber insurers are willing to take on the added risk of paying these fines is yet to be seen. Some have paid, while others have excluded these fines from their coverage.

STEPHANIE DINGMAN: A typical cyber insurance policy will address costs incurred following a cyber attack, including forensics costs, the cost of notifying those whose data has been breached, the cost to hire a PR agency to address reputational damage and credit monitoring for those affected.

Insurance can also provide coverage for extortion events, including ransomware attacks. It can also provide business interruption, extra expense reimbursement and cover potential third-party liability, including some regulatory action.

Firms also value cyber policies because they provide support and expertise as insurers work with their clients to assess and mitigate cyber risk.

Where do coverage gaps on current cyber policies exist, and what can organizations do to mitigate those gaps?

STEPHANIE DINGMAN: Typical insurance market cyber policies do not cover bodily injury and property damage, theft of first-party intellectual property, loss of sales due to reputational harm, real monies lost or loss of future investments. The marketplace continues to evolve but it's important to have a thorough gap analysis completed. This provides guidance on where there may be overlap with other policies such a property, crime, general liability and others.

> *Many colleges are racing toward cybersecurity to better meet the realized risks of staffing the next generation of cyber warriors. Consult CISOs, information security directors, analysts and ethical hackers in curriculum development."*
>
> — **BOB ECKMAN,** *Chief Information Security Officer,* MCPc

How will artificial intelligence drive the need for more secured Internet connected devices?

BOB ECKMAN: Technologists are still in the honeymoon phases of artificial intelligence. Currently, we are in a phase of understanding the data and cherry-picking the data that our AI solutions will consume. We are also tightly controlling the algorithms being used to evaluate and analyze this data. The "decisions," for the most part, are still man's to make.

What is yet to be seen is what will happen when AI is given the autonomy to determine its own data bed, and use cognitive learning to revise, and in some cases re-code, its algorithms to arrive at different conclusions. These systems will become like addicts, wanting to absorb any and all available data to arrive at a "better answer."

As this shift occurs, the Internet of Things will become a natural pipeline for this data. By feeding IoT data (both residential and corporate) into AI solutions, the industry will have the data fuel it needs to allow AI solutions to take control. This control will begin with everyday tasks and evolve overtime to include higher functioning activities like health care, air traffic control, law enforcement, etc. As we move from analysis to control, the impact of cyber compromise will elevate significantly.

JOE COMPTON: Endpoints that feed into AI processing systems are vulnerable and pose a risk of compromise. Amazon's Alexa was in the news because police want Alexa recordings it may have made at a murder scene. If you have an Alexa device, what could an attacker learn about you? If your water meter or electric meter were hacked, would an attacker know when you weren't home? What else could they learn?

How can educational and training programs address the increasingly sophisticated nature of cyber attacks?

STEPHANIE DINGMAN: Employees are perhaps an organization's greatest evolving security threat. To combat this, a consistent, frequent cyber-related campaign targeted at increasing employee awareness of cyber attacks is key.

A successful training program starts with support from senior leadership – companies must get understanding and buy-in by clarifying the business risks and consequences at the board level for potential data breach or cyber scenarios. Then, increasing employees' awareness of current cyber trends or threats and testing their ability to withstand "clicking on the link," including re-training for those who do click, is essential.

JOE COMPTON: First, the world needs more cybersecurity professionals. My company can't hire enough cybersecurity professionals to meet the market demand. We are currently having success with our internship program, and training folks right out of college, but it would be nice to find high quality experienced professionals who could step in and run projects. If you are in college, study MIS or computer engineering, you will always have a job waiting for you.

Second, general workers need regular IT security awareness training on a regular basis because the way cyber criminals attack is changing. Employees need to learn to spot social engineering attacks, and be trained to think twice before clicking on a hyperlink in an email or Word document.

I think for the most part, the training is catching up because there is a market for it. The challenge is giving people the tools they need to think critically and solve problems.

BOB ECKMAN: Many colleges are racing toward cybersecurity to better meet the realized risks of staffing the next generation of cyber warriors. All well intended.

When I'm not a CISO for a major tech firm, I also teach cybersecurity to undergrad, post grad and law students. This experience as an adjunct has served to give me a very specific view of this issue. Educators and administrators alike should resist the urge to develop these cyber programs in the vacuum of the purely theoretical.

Instead, and as someone who is on both ends of the workforce development pipeline, incorporate real-life security people in the curriculum development. Consult CISOs, information security directors, analysts and ethical hackers in curriculum development. Incorporate cyber labs and security operations centers that give students the ability to work side by side with cyber professionals testing, probing and developing cyber solutions. Allow these professionals to invite students to take part in the cyber community and learn the cyber methodology.

By incorporating practical, real-life experience, we not only show students that security can translate into a career, but we begin to graduate students who have real cyber experience and who can better appreciate the level of commitment required to be a cyber professional.

CRAIN CONTENT STUDIO
Cleveland

Advertising director: Nicole Mastrangelo, *nmastrangelo@crain.com*

Managing editor, custom and special projects:
Amy Ann Stoessel, *astoessel@crain.com*

Project editor: Kathy Ames Carr

Graphic designer: Staci Buck

For more information about custom publishing opportunities, please contact Nicole Mastrangelo.