CRAIN'S CUSTOM MEDIA
A DIVISION OF CRAIN'S CHICAGO BUSINESS

Advertising Supplement to Crain's Chicago Business

A ROUNDTABLE DISCUSSION

Cybersecurity

Advice for Preventing, Dealing with Breaches

As news about cyber crises breaks with increasing frequency, organizations and individuals everywhere are scrambling to protect data and personal information from hackers and others looking to do damage.

Crain's Custom Media asked three nationally recognized cybersecurity experts for their insights on how executives can prevent such breaches while protecting their businesses, employees, suppliers and customers.

Jerry Dixon

Chief Information Security Officer
CrowdStrike
jerry.dixon@crowdstrike.com
888-512-8906

Jerry Dixon is the chief information security officer at CrowdStrike, which provides endpoint security, threat intelligence and incident response services to customers in more than 170 countries. He has more than two decades of cybersecurity experience, including leadership positions at American Express as well as top-tier security companies and government agencies including the Dept. of Homeland Security and U.S. Computer Emergency Readiness Team. He's considered an industry expert on risk mitigation, incident response and proactive security.

William Dixon

Associate Managing Director - Cyber Security and Investigations
Kroll
william.dixon@kroll.com
213-443-1111

William Dixon is associate managing director of the cybersecurity and investigations practice at Kroll, a global provider of risk solutions with more than 35 offices in 20 countries. A 16-year information security services veteran, he held both technical and client management roles with Fortune 500 firms and start-ups before joining Kroll. He's served as a chief information security officer and as an advisor to boards of directors on cybersecurity and cyber threat awareness.

Michael Mantzke

President, CEO
Global Data Sciences Inc.
mantzkem@globaldatasciences.com
630-299-5196

Michael Mantzke is president and CEO of Global Data Sciences Inc., a business strategy and technology consulting firm that he co-founded in 2007. He's also the chief encryption architect for Encrypted Information Exchange, LLC, which develops messaging apps for desktops and mobile devices. Previously, he was chief information officer for Powermate Corp. and before that held numerous technology and engineering roles at Sunbeam Corp. His business career spans 35 years, with a lifelong passion for technology and innovation.

What role does your firm play in helping companies enhance cybersecurity?

William Dixon: Kroll helps clients respond to and prepare for cybersecurity events and incidents. We focus on helping clients minimize the impact of a cyber incident and serving as a trusted advisor in the event of an incident. Before an incident occurs, we help guide and build programs that protect organizations' digital assets, including infrastructure, applications and information. We've served as the lead on some of the largest data breaches in recent history and routinely advise boards on the importance and significance of a defensible cybersecurity program and approach that's attuned to their business and critical assets.

Michael Mantzke: Global Data Sciences embraces the complex topic of cybersecurity and presents it in a simplified format, helping companies understand its many layers and risks. We outline the necessary steps to diminish the threat, while defining policies and procedures to deal with the reality of a breach. One point we drive home to companies is that a breach will occur at some point; it's not so much a question of "if" but "when." Our goal is to create awareness for executives and develop sustainable plans to deal with the reality of the threat. We develop custom software solutions to secure users' data. One example is a messaging app we're developing featuring "encrypted transparency" â„¢ for secure mobile communications in the legal profession.

Jerry Dixon: CrowdStrike's the leader in cloud-delivered endpoint protection. Our CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints both on or off the network. For us, it's all about securing a company's brand, its data and its people. It's a responsibility we take seriously and it drives us to constantly push the envelope, hunt for new threats and adversaries, and devise better ways to stop them. As George Kurtz, CrowdStrike's CEO and co-founder, says, "We don't have a mission statement—we are on a mission to protect our customers from breaches."

What are some of the most common cyber threats you're seeing currently?

JD: Phishing is still a major problem for many organizations. It's easy for criminals or sophisticated actors to send massive numbers of emails to companies knowing that someone will click on them. Once they gain access, they can steal information or extort the company with ransomware. Another trend is attackers who add malicious code to open source software or a company's mobile applications, internal software or web applications so they can steal data or gain access to the company's network.

WD: I routinely see phishing as well as social engineering, where cyber extortionists target specific data within an organization, such as personal health information or financial data. These threats are then amplified in organizations that are behind in routine system maintenance and hygiene.

MM: The most concerning to me is the threat of infrastructure failure, which has become more prevalent in recent years. We're all too familiar with the data breach of large retailer customer information; it's in the news frequently. On the other hand, there are people issues: those unaware that their actions—such as leaving their mobile devices or computers unlocked while unattended—contribute to the cybersecurity problem. Employees willingly provide personal information when asked by store clerks, or even over the phone. This lack of diligence contributes to the cybersecurity problem.

What are some typical cybersecurity shortcomings you see in businesses when you begin working with them?

MM: The most prevalent shortcoming is executives who don't take cybersecurity seriously—or worse, are dismissive. I've heard executives say, "My IT guys have it under control," or "Our banks have us covered," or my favorite, "What are the odds we are a target?" That default response sees many executives dump the issue in the lap of an IT department treated as a utility rather than as a strategic partner in the minds of business executives.

JD: Many organizations lack a comprehensive cybersecurity crisis management plan, and if there is one, not everyone in the organization's aware of it. They should rehearse it on a quarterly basis with senior leaders across the organization. Another challenge for many organizations is lack of visibility into their information technology enterprises, including endpoints and servers.

WD: Companies don't always understand what information they're trying to protect. They do a good job identifying specific processes or applications they want to protectÂ—such as email, a web application, etc.—but they aren't sure of the exact significance. Another shortcoming is user awareness and training. The biggest return a company can get on its security investment is the protection that can be provided by its employees.

What are some do's and don'ts for companies responding to data breaches?

WD: The most significant "do" is patience—take the time to get all the necessary information together to construct a timeline and story about what systems, applications, data and processes were impacted. Once that's done, the threat can be removed from the environment and other key questions can be answered. The biggest "don't" is approaching an incident from a position of shame or failure. Don't let emotions or a feeling of failure about being a victim impact a solid response.

MM: Don't take anything for granted. Don't assume anything. Do treat any cyber breach as a threat. In the case of data loss, ensure the latest system backups are secure. When a breach is detected, follow defined business policies and procedures to ensure compliance measures are being followed. And follow all legal and compliance guidelines regarding notifying impacted agencies and individuals. Determine how the breach occurred, and what staff or contracted resources were responsible. Don't hide from the reality. Something failed—find out what and fix it.

JD: Have a data breach response plan in place that's been regularly rehearsed and that people can follow. There are many moving parts, from managing legal and regulatory risk to communicating with a board of directors, customers and business partners. It's crucial to have the general counsel involved, and if there's a cybersecurity firm on retainer they can investigate, provide an independent assessment of the breach and help coach internal security teams. Don't externally communicate specific details within the first 24-48 hours.

What's your advice regarding cyber liability insurance?

JD: All organizations should have cybersecurity insurance due to recovery cost, business impacts and legal risk associated with a data breach or network intrusion. Cybersecurity insurance also provides response coaching, pre-approved firms for conducting the breach investigation, outside counsel and other support services that will help minimize the impact. Many larger companies are now requiring suppliers or business partners to carry a certain level of cybersecurity insurance to help minimize their overall liability for a
data breach.

WD: Cyber liability insurance should be part of a defensible cybersecurity program portfolio. At a minimum, the policy should cover multiple types of events and incidents, and have cohesion with a company's other insurance products since it's rare that only a cyber policy is invoked in the case of an incident. Businesses should also assess where they may have gaps in their risk management approach to help determine any exposure they weren't even aware of.

MM: While insurance provides a safety net, it can't make up for weak policies or employees who keep passwords on a post-it note next to their computer. That's why it's critical that businesses match their external insurance policies with internal best practices. Outlining clearly—for employees of every level—the importance of securing data and the ways to do so is paramount.

What initial steps should a company take if it wants to invest in a cybersecurity program?

WD: The investment should start with people, making users and employees aware of the significance of the information they deal with on a daily basis, and what methods can be used to extract and misuse it. At the most basic level, it takes the form of a policy and ongoing user awareness, training and testing to gauge the effectiveness of employees in preventing a cyber incident. At Kroll we've designed such programs, and work with clients to identify the right mix of technology and services that make the most sense for the industry and in some cases, budget.

JD: The first step is to designate a chief information security officer (CISO) to be the point person for managing risk and driving response activities, including security awareness and compliance. The CISO should develop a risk register that accounts for the types of risks that can affect the confidentiality, availability or integrity of systems, applications or data. He or she can work with the company's business units to identify which risks are business-impacting, then develop a plan to reduce the risk. The CISO should also develop metrics for demonstrating the effectiveness of the information security program and present them quarterly to the company's board and other top leaders. One tactic that can fast-track a cybersecurity program is to have an outside firm conduct a security assessment of the company, including a simulated attack against the organization. These can shine a light on any areas that need to be quickly fixed.

MM: Companies should focus on the following key areas: compliance requirements for their specific industry; business infrastructure component maintenance; threat assessment management; encryption protocols for data sharing; and GEO-locking protocols, in the event devices are removed from sensitive business networks.

What's your view about cybersecurity protection for key executives and board members?

WD: Directors and executives wear multiple hats. One is that they're accountable for the actions and effectiveness of their organization's cybersecurity program. This has caused the board and executives to take a significant interest in the activities and effectiveness of what the organization is doing to minimize the impact in the event of an incident. That being said, individual protection and assessment of the boards and executives' individual cybersecurity posture is important and we're seeing many executives and board members assessing their own personal and home cybersecurity postures to close any gaps that could allow bad actors access to their information and assets.

MM: Cybersecurity protocols and policies only truly work when they're implemented and followed at every level—from entry-level associates to key executives. That same rule extends to board members who also have access to information that must be kept secure. Board members must be brought into the system so they can understand and abide by companies' cyber policies and procedures.

JD: While companies often invest in physical security protection for their key leaders, they often overlook cybersecurity protection. Yet they're frequent targets of competitors, nation-state governments, criminals, or insiders wishing to gain access to their computers or data. These business leaders often travel abroad where physical risk increases but so does cybersecurity risk. Both the physical security and cybersecurity teams should work together to brief executives and board members about the types of risks they face when traveling and how they can protect themselves. We often teach them street smarts when traveling but we also need to teach the senior leaders digital street smarts.

As the Internet of Things (IoT) continues to grow, what potential cybersecurity challenges lie ahead for businesses?

MM: My greatest concern is the lack of discipline in the emerging application development community. Not all IoT apps are created equal with regards to cybersecurity. Because the apps are available for installation by employees using their personal phone for company business, they potentially open up a pathway to company data and company infrastructure. As a business culture, we've sacrificed security for simplicity and ease of access, and have left the door wide open for cyber attacks.

JD: Security cameras, building access control systems, cooling or heating systems, power distribution systems and connected devices all expand the attack surface of a company. Attackers are already taking advantage of these connected devices because they were often built with minimal security controls. As a result, traditional security perimeters for businesses are rapidly disappearing and organizations are having to move into a new security paradigm called zero-trust networks.

WD: Challenges will come in the form of having better network intelligence and understanding that intelligence. Many IoT devices can't be monitored on the device itself, so the networks that they reside on need to be designed and monitored in such a way that data being directed to the device and data being generated by the device can be tracked and understood. Monitoring the network is going to be the most important aspect to securing IoT, which may require segmenting out devices so they all reside in a known part of the network.

Crain's Chicago Business | Privacy Policy | Contact Us