EXECUTIVE ROUNDTABLE
Sponsored by Rapid7

Accelerating Incident Response: Organizational Shifts for Faster Remediation

Agenda

6:00 – 6:30 p.m.
Networking & Cocktails

6:30 – 6:45 p.m.
Introductions and Opening Remarks

- **Nick Holland**, Director, Banking and Payments, Information Security Media Group
- **Scott King**, Senior Director, Security Advisory Services, Rapid7

6:45 – 8:15 p.m.
Roundtable Discussion

8:15 – 8:30 p.m.
Closing Remarks

8:30 p.m.
Program Concludes

ISMG INFORMATION SECURITY MEDIA GROUP

RAPID7

Introduction

Data is the most valuable asset for any organization, and time lost between compromise, detection and response to cybersecurity intrusions can mean critical – even existential – damage to businesses. Yet many organizations are still struggling to implement a cybersecurity incident response function into their business operations.

How can today's cybersecurity teams better integrate incident response into operations? And how can cybersecurity, IT and OT teams find common ground?

This executive roundtable on **Accelerating Incident Response: Organizational Shifts for Faster Remediation**, will provide answers to these and other questions. Scott King of event sponsor Rapid7 will provide strategic insights on how business growth can be protected in today's cybersecurity threat landscape.

This invitation-only dinner will also draw from the experiences of the attendees, who will share their views on how business growth can be protected in an era of cyberattacks.

Among the discussion topics:

- To what degree are your cybersecurity incident response and business response postures integrated?
- What kind of organizational structures work best for ensuring rapid incident response?
- How can an organization win board-level buy-in for the need for a holistic incident response plan?

You'll have the opportunity to discuss the topic with a handful of senior executives and market leaders in an informal, closed-door setting, from which you will emerge with new strategies and solutions you can immediately put to work.

Discussion Points

Among the questions to be presented for open discourse:

- To what degree are your cybersecurity incident response and business response postures integrated?
- Where are you on your road to getting IT and OT teams to speak a common language?
- How do you rate your organization's ability to meet today's incident response needs?
- How can an incident response posture and an overall disaster response plan be better aligned?
- How can an organization win board-level buy-in for the need for a holistic incident response plan?
- What kind of organizational structures work best for ensuring rapid incident response?
- What technologies are paving the way for a more effective incident response strategy?

About the Expert

Joining our discussion today to share the latest insights and case studies is:

Scott King

Senior Director, Security Advisory Services
Rapid7

King has over 20 years of experience in the IT and cybersecurity fields. He started his career as a network and systems engineer, and then moved into an information assurance role supporting the Department of Defense, which kick-started his career as a cybersecurity professional. King has worked extensively in the energy industry, DoD, state governments and at technology and manufacturing companies. He brings a mixture of hands-on experience in incident response, penetration testing, forensics, SecOps, architecture, engineering and executive leadership as a former CISO.

About Rapid7
Rapid7 (Nasdaq: RPD) is advancing security with visibility, analytics and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks and automate routine tasks. Over 7,900 customers rely on Rapid7 technology, services and research to improve security outcomes and securely advance their organizations.

About the Moderator

Leading our discussion today is:

Nick Holland

Director, Banking and Payments
Information Security Media Group

Holland, an experienced security analyst, has spent the last decade focusing on the intersection of digital banking, payments and security technologies. He has spoken at a variety of conferences and events, including Mobile World Congress, Money2020, Next Bank and SXSW, and has been quoted by The Wall Street Journal, CNN Money, MSNBC, NPR, Forbes, Fortune, BusinessWeek, Time Magazine, The Economist and the Financial Times. He holds an MSc degree in information systems management from the University of Stirling, Scotland.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from the North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

For more information, visit www.ismg.io.

CONTEXT

Accelerating Incident Response: Organizational Shifts for Faster Remediation

Q&A with Rapid7's Scott King

NOTE: In advance of this event, ISMG's Nick Holland spoke about accelerating incident response with Scott King. Here is an excerpt of that conversation.

Common Missteps

NICK HOLLAND: What are the most common missteps that you see today when it comes to aligning incident response with business response in organizations?

SCOTT KING: More often than not, cybersecurity incident response teams work in a silo, monitoring, analyzing and responding to events. This approach works when the events turn into small incidents and do not require much intervention from IT or the business. However, that approach leaves some large gaps when the event turns into a larger incident that impacts the business and requires more people and functional areas to all be working in unison.

This challenge is compounded when other departments have differing objectives and IT generally gets caught in the middle with no one really in charge of the incident.

As businesses grow, the need for specific crisis response plans becomes paramount in order to manage a wide range of business impactful situations, such as natural disasters, safety impacts, and power outages. Just like other business impacts, cyber incidents introduce issues that can shut down the company's IT systems, expose data, and cause negative reputational issues. Those impacts quickly turn into a crisis. And without a prepared, trained workforce with a rehearsed plan, the likelihood of minimizing the impact from cyber incidents increases dramatically.

Teamwork

HOLLAND: Cybersecurity is traditionally seen as a contradictory force to operations. How can the two teams work together when it comes to incident response?

KING: This is an interesting challenge. Cybersecurity functions are often designed to put barriers in place separating "acceptable" technology usage from those deemed "unacceptable."

What is considered acceptable varies between companies and even between different departments in the same organization.

"Cybersecurity functions are often designed to put barriers in place separating 'acceptable' technology usage from those deemed 'unacceptable'."

Insert mandatory regulatory requirements governing technology operations and cybersecurity investments and you quickly see a slowdown to free-flowing technology use that is generally viewed as a business enabler.

For risk-driven businesses, this is less of a concern, as the risk or safety culture has informed worker expectations that productivity impacts are the cost of doing business. For most businesses however, those impacts are not as acceptable, and the workforce has an expectation they can do generally what they want, regardless of the risk it introduces. In those situations, where preventive and more restrictive security controls are not part of the risk-management strategy, the cybersecurity team is left with their fall-back controls, monitoring and incident response.

Regardless of the risk equation though, the incident response process becomes a win/win where business, IT and cybersecurity functions have to all work together to ensure the company is well-prepared to manage a cyber incident and resume normal business in the shortest time possible.

C-Suite Awareness

HOLLAND: Do you think today's C-level executives are sufficiently aware of the damage that can occur from an ineffective incident response strategy?

KING: In short, no. The majority of C-level executives understand that cyber is an area that can bite in specific ways, but few truly understand or ask about how well prepared the company is to respond to a cyber incident that impacts its ability to function. Those that do understand are often surprised that they are not well-prepared to handle a massive IT outage or data breach due to a cyber incident. This can be attributed to a variety of factors, none of which are helpful to ensuring business can return to normal operation quickly after a cyber incident.

> "Rapid7 is uniquely positioned to help organizations of all sizes and industries understand and manage their cyber risk."

Three Key Steps

HOLLAND: What three things could organizations do to educate the importance of everyone's role in timely incident response to their employees?

KING: First, the leadership team of the organization needs to determine their risk tolerance to business impacts. Specifically, how much lost productivity is acceptable and how much financial liability can be assumed? Once those norms are established, an enterprise risk team (or board committee) can measure different departments and business functions based on key risk indicators, which informs the cyber investment strategy.

Second, the cybersecurity team must work outside the silo security often enables and engage with both the business and IT to focus on ensuring the risk tolerances are managed through process and IT operations. This will result in role definitions and an appreciation for how teams must work together in the face of increasing cyber incidents.

Lastly, once there is clear line of sight to how risk is managed and the roles of the business, IT and cybersecurity are defined, incident response plans, training and practice can be achieved. This last part is the culmination of a significant amount of work and decision making, which all goes into minimizing the impact and expedites the recovery from a cyber incident.

Rapid7's Role

HOLLAND: How can Rapid7 aid organizations manage their risks?

KING: Rapid7 is uniquely positioned to help organizations of all sizes and industries understand and manage their cyber risk. Through the technology products, managed services and consulting services we offer, businesses can leverage us as a partner that will help them with their entire cybersecurity ecosystem. ■

Notes

Notes

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io