CLOSING THE GAP ON BREACH READINESS

INSIGHTS FROM THE SECURITY FOR BUSINESS INNOVATION COUNCIL

OVERVIEW

This e-book contains insights on breach readiness, response and resiliency based on in-depth interviews conducted with the Security for Business Innovation Council (SBIC)[1]. The SBIC is comprised of forward-thinking security executives from Global 1000 enterprises committed to advancing the state of information security worldwide by sharing insights from their real-world experience.

Readiness benchmarks for the industry at-large are drawn from a global survey of 170 security practitioners in 30 countries. Measures within four major areas of breach readiness and incident response are provided: Content Intelligence, Analytic Intelligence, Threat Intelligence and Incident Response.

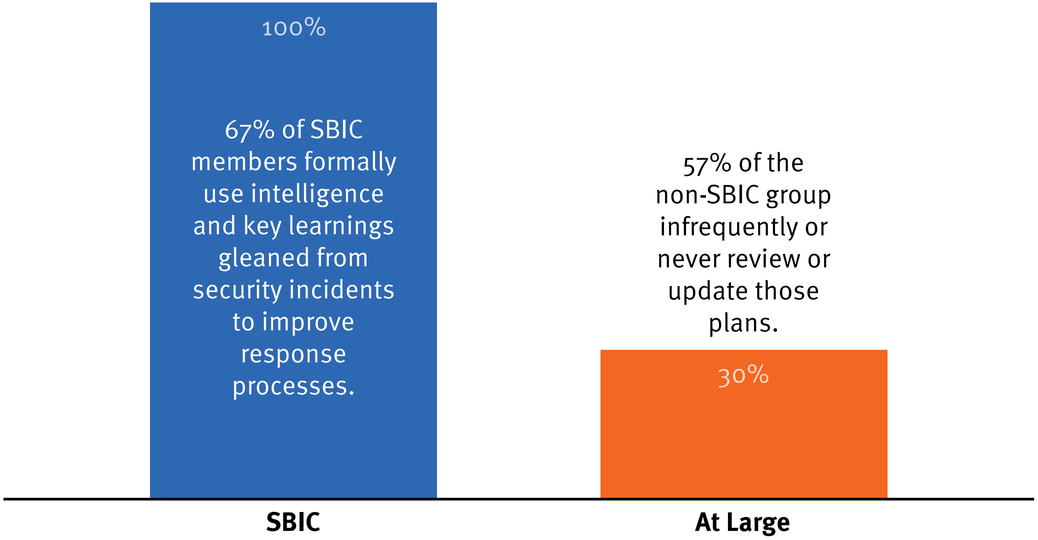
By comparing and contrasting the responses of industry leaders with the industry at-large, we are able to offer actionable recommendations for building a pre-emptive breach readiness and response program.

[1] See addendum for complete list of SBIC organizations and representatives

INCIDENT RESPONSE

Incident Response is a comprehensive, premeditated approach to protecting applications, data and information infrastructure from cyber attacks. Process, people, procedures and technologies are core elements of a thoughtful incident response plan.

Incident Response planning is dynamic. Enterprises that fail to evaluate Incident Response plans against new threats expose their systems, data and infrastructure to attack.



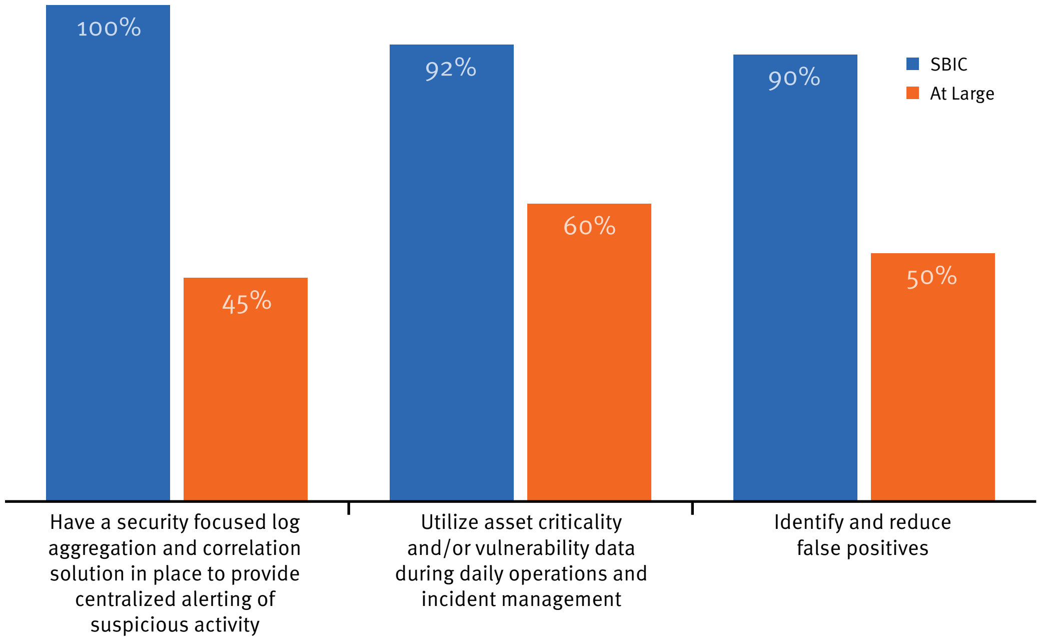
Have formal Incident Response plans in place.

> “People and process are more critical than the technology as it pertains to incident response. First, a security operations team must have clearly defined roles and responsibilities to avoid confusion at the crucial hour. But it is just as important to have visibility and consistent workflows during any major security crisis to assure accountability and consistency and help organizations improve response procedures over time.”
>
> *Ben Doyle, Chief Information Security Officer, Thales Australia and New Zealand*

CONTENT INTELLIGENCE

Content Intelligence is a state of situational awareness gained from the tools, technology and processes organizations have in place to identify and monitor critical assets and disseminate actionable intelligence for analysis and response

SBIC members have skilled cyber security teams tasked solely with identifying and implementing technologies for heightened Content Intelligence. Information sharing is an institutionalized and ongoing process.

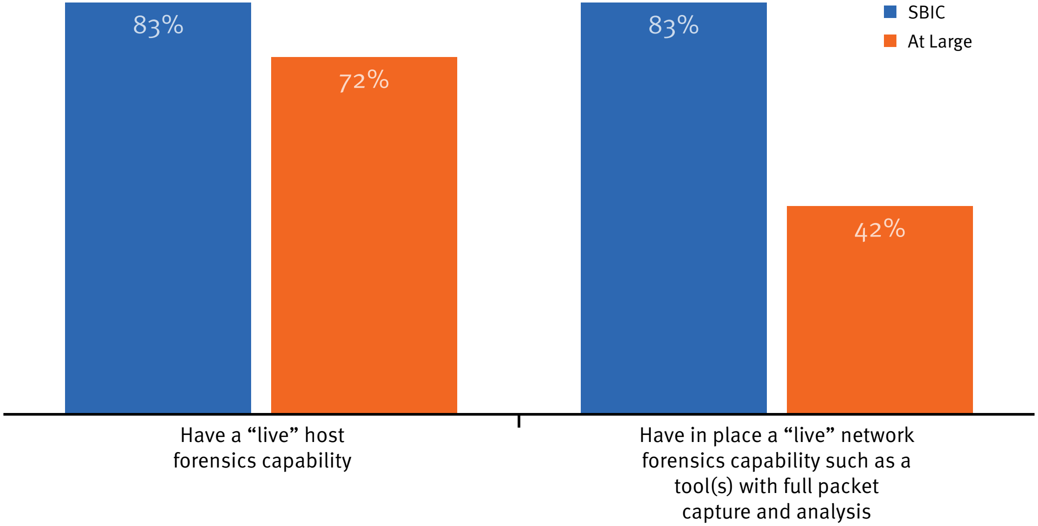


> **“Organizations need to continually refine their approach to intelligence collection. How timely and actionable is it? Is it valuable to the business? Without doing so we will be overwhelmed with information and virtually lost”**
>
> *Tim McKnight, Global Chief Information Security Officer, General Electric*

ANALYTIC INTELLIGENCE

Analytic Intelligence is a forensic – or post-event – threat analysis.

Understanding how malware operates and what systems it targets is essential to developing threat intelligence, incident response, and bolstering cyber security defenses.

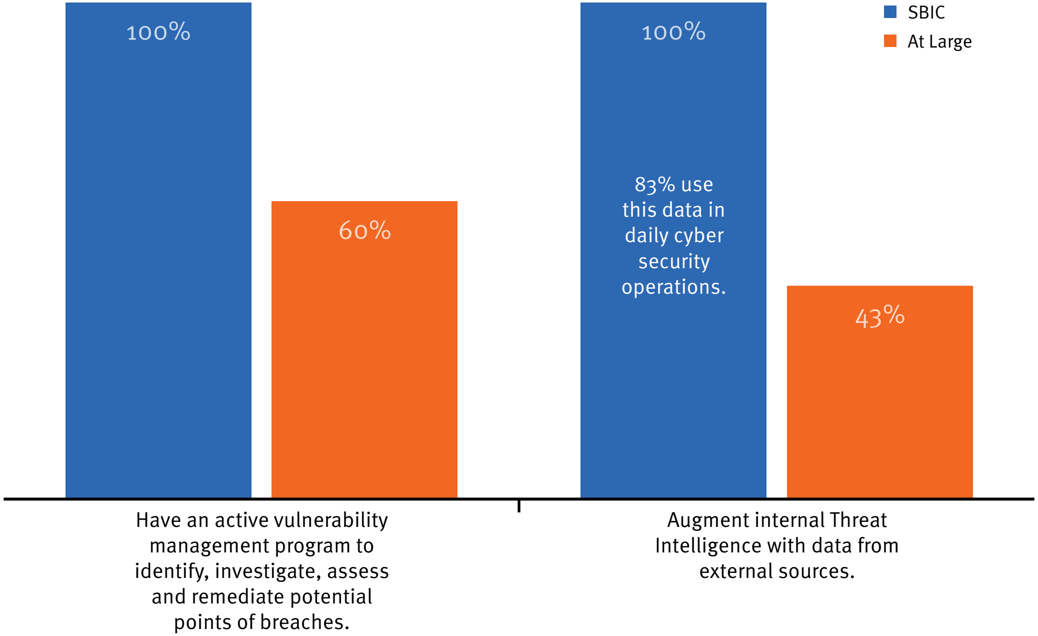


> "It is important to use both internal and external sources for malware detection and analysis. By using third parties, organizations can see more of what is going on and leverage that intelligence to prepare for future attacks."

Dave Martin,
Chief Trust Officer, RSA

THREAT INTELLIGENCE

Threat Intelligence is the process of collecting and synthesizing internal and external threat data to implement effective detection, investigation, and response to security events



> **"Security Operations must maintain a certain level of flexibility. With zero-day events and other types of attacks that are less understood, security operations teams must be nimble and adaptive. Subscription based services are good for additional help if your team is resource constrained."**
>
> *Jerry Geisler, Senior Director, Information Systems Security Operations, Office of the Chief Information Security Officer, Walmart*

ADDITIONAL INSIGHT

BEST PRACTICES

CONTENT INTELLIGENCE

Establishing content intelligence is critical and the first step to building a breach readiness and response program. The following steps are fundamental starting points:

Leveraging security information and event management (SIEM) technology to detect anomalies with a dedicated resource or team to analyze potential incidents

Cross-referencing all anti-virus and firewall logs with detected incidents

Incorporating asset vulnerability data into the SIEM

This is an ongoing process. SBIC members, who have advanced breach readiness and response protocols in place, advocate continuous improvement. Fifty eight percent of members interviewed stated that despite having central aggregation for security logs and alert automation, it is difficult to ensure coverage for all critical assets.

False positives are another challenge. Analyzing false positive incidents enables adjustment of SIEM systems. Among SBIC members, 50% lack a formal process. Many enterprises are not thinking about false positives.

At the highest level of breach readiness and response, organizations move security operations from being a siloed risk function at the IT or Security departmental level to become part of the larger operational risk view. Consider the multitude of high-profile breaches over the past year, and it is clear that all areas of the business must have a stake in information security. According to SBIC members, data sharing among internal teams is critical whether through regular out-of-band communications or centralized Governance, Risk & Compliance (GRC) .

ANALYTIC INTELLIGENCE

Malware analysis is standard forensic technique fundamental to breach readiness and response. By understanding how malware operates and what it targets, organizations can network and endpoint vulnerabilities to improve attack detection and defense.

Forensic tools for static and dynamic analysis of memory usage, open network connections, running processes, and event logs can reveal evidence of stealth attacks and intrusions. Eighty-three percent of SIBC members have a live host and network forensic capabilities; although these tools are deployed at various levels of functionality and not all are using them in the investigative process.

BEST PRACTICES

THREAT INTELLIGENCE

Vulnerability data combined with advance determination of information asset importance (for example, Mission Critical, Business Critical)gives business context that helps organizations prioritize resource allocation for prevention and incident response. According to the SBIC, the following threat data should be mined to improve breach readiness and response:

- Vulnerability data
- Open source threat data
- External threat intelligence feeds from third parties

INCIDENT RESPONSE

According to the SBIC, at heart of effective breach response is a full-time, dedicated security operations staff. This team should have clearly defined management roles in one of three areas: Security systems: intelligence and incidents, and: security data and analysis.

Understanding that IT security and cyber security require different abilities is an often overlooked distinction. Cyber security and information security are related but distinct disciplines. Both protect information systems, but the purview of cyber security extends beyond networks and systems to asset classes such as strategic infrastructure. Cyber security is also more proactive. There are other qualifications cyber security professionals must possess that are not required of traditional IT, including an understanding of business processes, the ability to gather, analyze and act on intelligence, and a deep understanding of the entire organization in which they operate

How security incidents are prioritized and tracked can dramatically impact the effectiveness of breach response. Many organizations still rely on a manual, decentralized system for tracking security incidents In some cases, this consists of little more than a spreadsheet updated by security analyst on an ad-hoc basis. This makes it difficult to provide governance, track how incidents are being addressed, and offer insight into process improvement over time.

Organizations should employ a dedicated workflow-based system that provides full visibility – from alert collection to incident creation and escalation through mitigation, containment, analysis and remediation. Among SBIC respondents, only 58% employ a dedicated incident and workflow management system for security operations to track and manage incidents.

Lastly, regular testing increases the chance that incident response procedures will deploy as planned when required. Among SBIC members, 92% have a formal process in place to test their incident response program at least once a year. Cyber war games identify areas for improvement and ensure the right levels of attention, staff and budget are focused on its highest-value applications and data and vulnerable infrastructure.

IS YOUR ENTERPRISE BREACH-READY?

Essential Questions in the Four Major Breach Readiness and Response Categories

Content Intelligence

- Does your organization currently have a security focused log aggregation and correlation solution in place to provide centralized alerting of suspicious activity?
- Does your organization have a dedicated team/function for the development and testing of new content for security technologies such as SIEM?
- Are detected incidents cross-referenced with your organizations antivirus logs to improve content intelligence?
- How prepared is your organization to address a significant security breach if one were to occur today?
- Do you have measures in place to identify and reduce false positives produced by your automation technologies?
- Does your security organization share data between the risk function and the security operations function?

Analytic Intelligence

- Does your security organization currently have a malware analysis and/or a reverse engineering function?
- What type(s) of malware analysis capabilities exist within your organization?
- Do you currently have a “live” host forensics capability?
- Do you currently have in place a “live” network forensics capability such as a tool(s) with full packet capture and analysis?

Threat Intelligence

- Does your security team review threat data to categorize and prioritize the data for use in daily operations?
- Does your organization have a vulnerability management program?
- Does your security operation program utilize open source threat intelligence data for use in daily operations?
- Does your security operation program purchase external threat intelligence data for use in daily operations?
- Does your organization regularly analyze lessons learned from security incidents to generate intelligence that is fed back into security operations for continued refinement?

Incident Response

- Does your organization have a formal Incident Response procedure?
- What is the structure of your incident response team?
- Do you have a system that enables your staff to prioritize their response to incidents?
- If your organization was notified by a third party, such as law enforcement, about a security breach within your network, do you know what steps are required to respond?
- How often are your incident response capabilities formally tested?
- How prepared is your organization today to address a significant security breach

SECURITY FOR BUSINESS INNOVATION COUNCIL

Marene Alison* — World Wide VP of Information Security, Johnson & Johnson

Anish Bhimani* — Chief Information Officer, Commercial Banking, JP Morgan Chase

William Boni — Corporate Information Security Officer (CISO) and Vice President, Enterprise Information Security, T-Mobile USA

Roland Cloutier* — Vice President, Chief Security Officer, Automatic Data Processing, Inc.

Dr. Martijn Dekker* — Senior Vice President, Chief Information Security Officer, ABN Amro

Ben Doyle* — Chief Information Security Officer, Thales Australia and New Zealand

Jerry R. Geisler III* — Office of the Chief Information Security Officer, Walmart Stores, Inc.

Malcolm Harkins — Vice President, Chief Security and Privacy Officer, Intel

Kenneth Haertling* — Vice President and Chief Security Officer, TELUS

Dave Martin* — Former Vice President & Chief Security Officer, EMC Corporation, Chief Trust Officer, RSA

Timothy McKnight* — Global Chief Information Security Officer, General Electric

Kevin Meehan* — Vice President and Chief Information Security Officer, The Boeing Company

Philip Hong Sun, Kim — Executive Vice President and Chief Security Information Officer, Standard Chartered Bank of Korea

David Powell — Head of IT Security, National Australian Bank

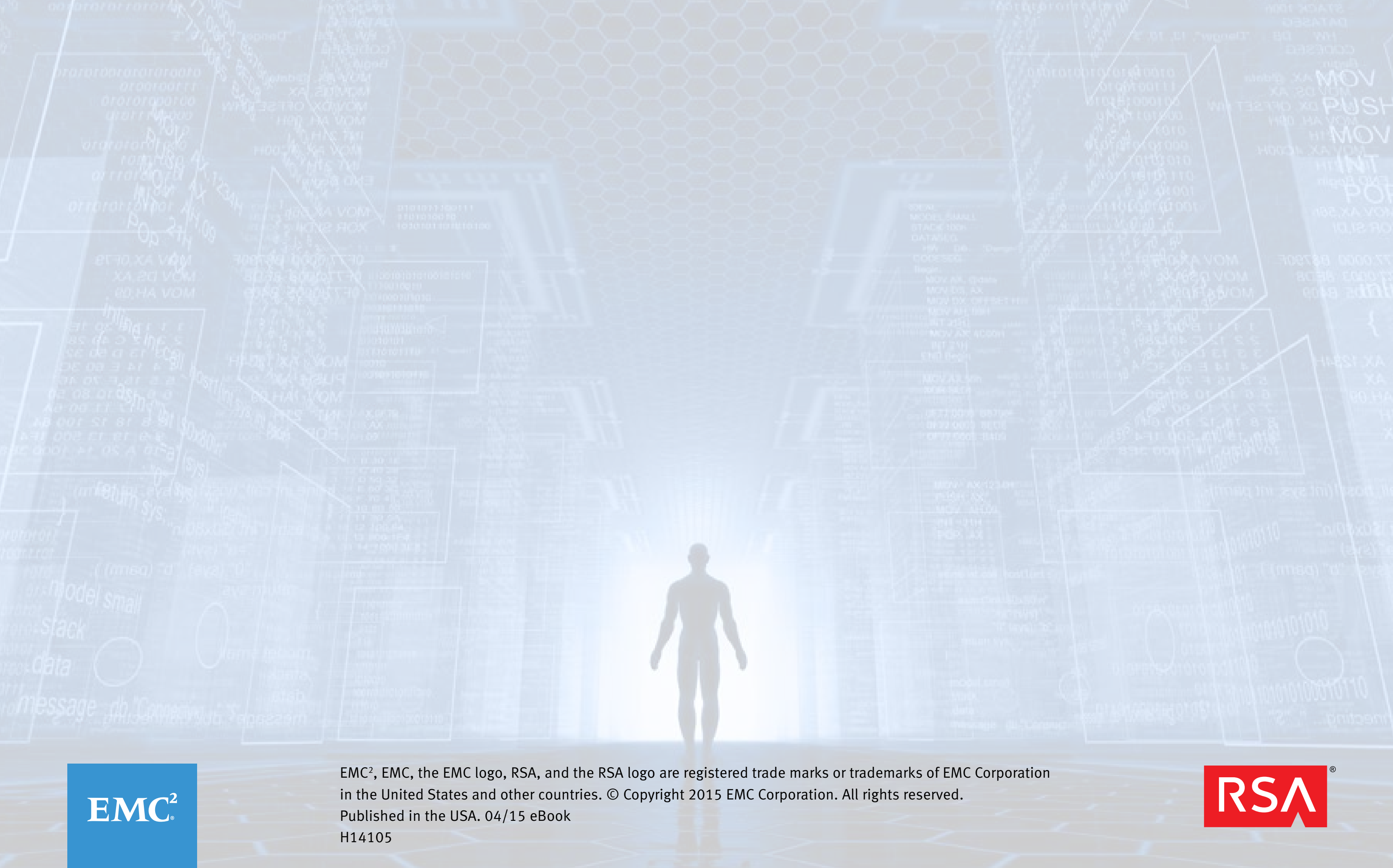
Robert Rodger — Group Head of Infrastructure Security, HSBC Holdings plc.

Ralph Salomon — Vice President Security, Processes & Compliance Office, SAP Cloud and Infrastructure Delivery

Vishal Salvi* — Chief Information Security Officer and Senior Vice President, HDFC Bank Limited

Denise D. Wood* — Corporate Vice President, Information Security, Chief Information Security Officer, Chief IT Risk Officer, FedEx Corporation

*SBIC members who participated in this survey



Published in the USA. 04/15 eBook
H14105