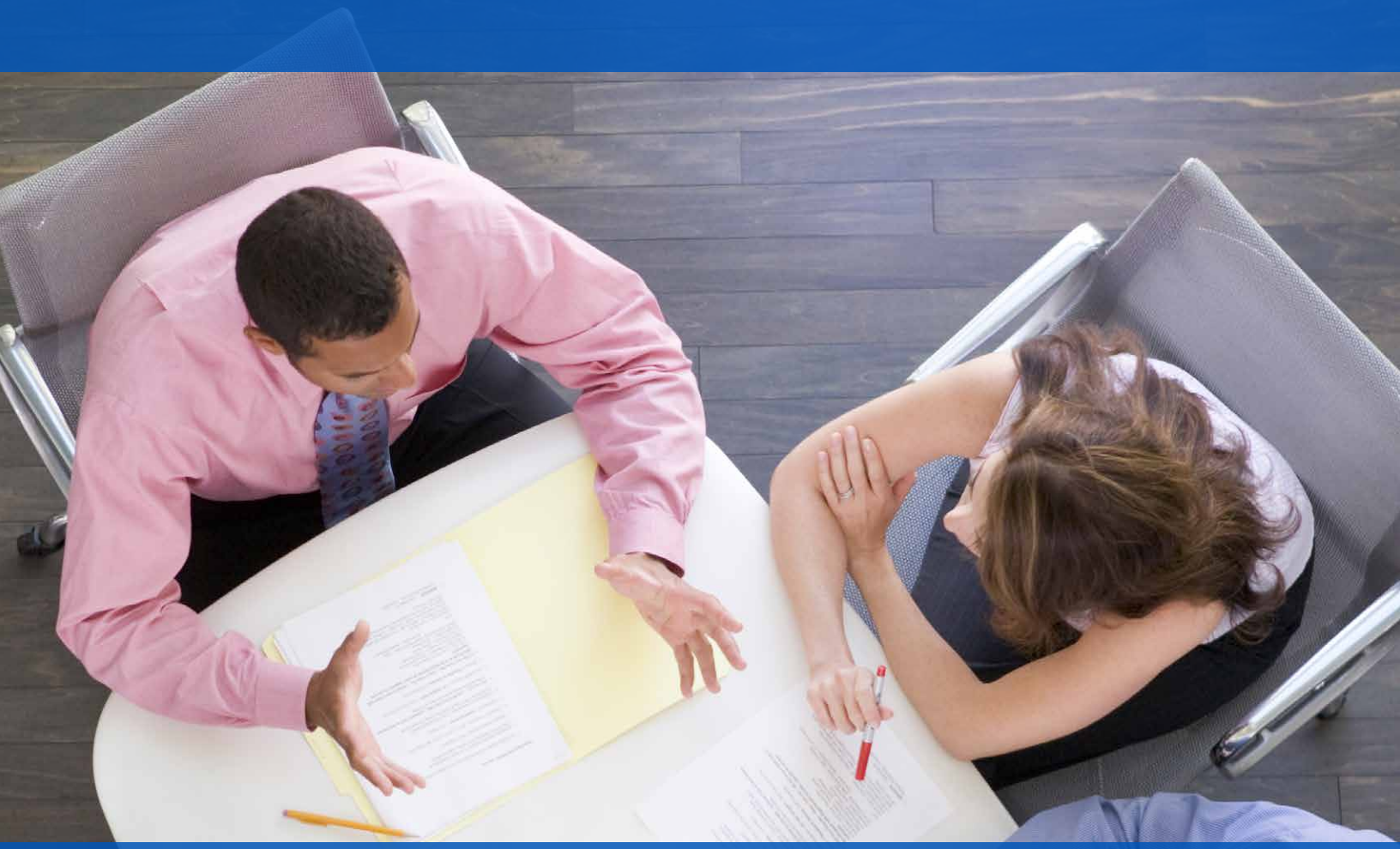
OPTIV



SECURITY INCIDENT MANAGEMENT

Solution Primer

Jenn Black
Senior Research AnalystSolutions Research and Development
Office of the CISO, Optiv

Introduction

Today, the capability to respond effectively to cyber incidents is one of the most critical components of an enterprise security program. A growing rate of breach disclosures in the news serves as proof that for most organizations, breaches are inevitable. For organizations of all sizes to survive these public debacles, they must enhance incident response capabilities as part of a principal investment in their security incident management program. The alternative is to risk damage to brand reputation, customer experience and loyalty, and profitability.

Many enterprise security programs continue to focus on prevention-based point solutions. Even security organizations looking to invest in more advanced programs such as threat intelligence still do so within the context of preventing attacks. While a few mid-market organizations have proposed to discontinue all prevention investment in favor of a combination of forensic retainers and cyber insurance, this strategy is not financially viable. The most effective approach, based on Optiv's primary research, is to:

- Increase operational security focus on incident response activities.
- Redistribute cyber security investment to include detection and response capabilities and resources.
- Create a business-aligned enterprise security incident management program.

Today's enterprises need to prepare on a broader scale to endure a breach. Applying a programmatic approach to managing cyber security incidents demands the involvement of more than security teams. In the persistent effort to maintain brand integrity and profitability, a structured, well-orchestrated response to cyber security incidents supports a more resilient business.

Meeting Business Needs

An enterprise-wide security incident management program is aligned with legal, regulatory and fiduciary customer responsibility and supports planning and testing a proactive incident response (IR) plan.

IR plans offer a coordinated approach to remediating incidents. Further, these plans support the business in taking legal action against malicious parties. On the flip side, IR plans can help protect executive leadership and the business against derivative lawsuits or regulatory inquiries. By creating and testing IR plans, executives demonstrate commitment to their fiduciary duties of due care, good faith and loyalty to the corporation and its shareholders.[1] IR plans also fulfill requirements for cyber insurance protection (and payouts).

It is also worth noting that the latest "Cost of Breach" report (Ponemon/IBM, 2015) [2] found that companies with designated IR teams decreased the cost of responding to incidents by eight percent ($12.60 per record).

Incident Management Defined

While security incident management has been defined in many different ways, Optiv defines Incident Management as:

> *"Incident Management (noun) – A security-centric program designed to prepare and orchestrate all aspects of the business in responding to a cyber security incident."*

Operationalizing Incident Management

Program Drivers

Program drivers are the reason(s) for the investment of company resources into defining, designing, deploying and maturing a security incident management program. These are the guiding principles of the security incident management program.

From our research, these are the main business justifications for investing in a security incident management program:

- Operational risks to the business from cyber breaches and attacks.
- Reputational damage and financial impacts.
- Compliance to regulatory, insurance and legal (law enforcement) requirements.

Business Requirements

Operating a successful security incident management program begins with understanding and meeting business requirements. Drivers help guide program development, business requirements define stakeholder expectations and objectives.

Although business requirements can depend on an organization's industry and market-segment, these three requirements (below) apply universally. Stakeholder expectations of the security incident management program included the following:

- Manage business impact (operational, brand, financial and others) posed by cyber security incidents and attacks.
- Manage organizational and fiduciary responsibilities for compliance, notifications and disclosures.
- Support the primary line of business and contribute to organizational value strategies.

Leveraging an Incident Management Program

The primary function of a security incident management program is to effectively manage the impact of cyber incidents on the primary line of business. As already discussed, "business impact" takes many forms beyond the technical and operational. Financial impacts must include cost of investigations as well as customer churn, penalties, litigation and other related costs. The security incident management program is expected to protect key operational processes, applications and data for conducting primary lines of business.

The primary function of a security incident management program is to effectively manage the impact of cyber incidents on the primary line of business.

Another critical requirement is accountability and ownership of compliance requirements for breach notifications and disclosures. Coordination with legal counsel and other parts of the business (finance, accounting, audit, HR) becomes critical in supporting this requirement. Technical investigations to determine attack patterns and responsible parties, whether data was exfiltrated, what type of data (if any) was exfiltrated, when the attack began and other elements impact organizational fiduciary duties for disclosures and notifications. With the number of internal groups involved in determining and meeting these requirements, a functional owner becomes a key requirement for the business.

Security leaders are being looked to for sufficient performance measures and changes to the overall threat landscape. Key performance indicators must be developed to demonstrate program efficacy. These may vary depending on audience. Tying performance to financial impact to the business is critical for senior and executive-level leadership. Business managers may be most interested in numbers of incidents detected in their particular division and how that may change over time and with appropriate training. Effective performance measures are critical to drive ongoing, iterative program improvements.

Developing a Program Strategy Approach

The foundation of any well-orchestrated security program is a strategy rooted through business alignment and supported by an appropriate balance of personnel, process and tools. Without an appropriate alignment to business objectives and available resources, the program will be unbalanced and produce irrelevant results.

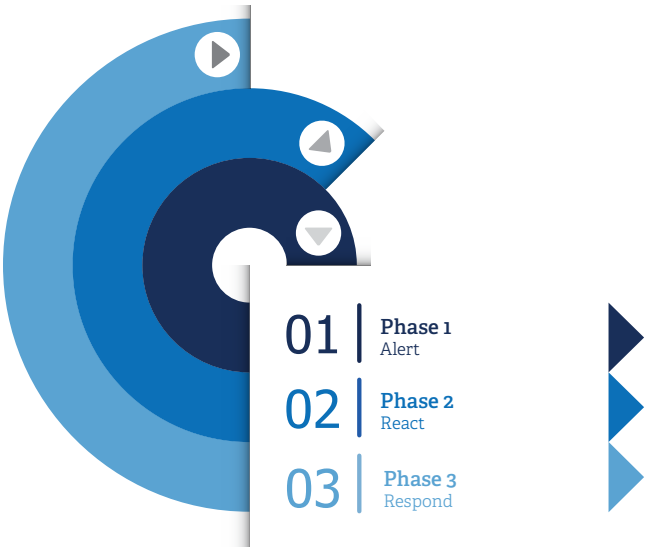
From Optiv's research, executives' expectations of security incident management programs are mostly under-reaching. While many are investing (or planning to) in additional response capabilities, executives expressed some doubts in achieving their security program's goals.

Here we discuss a three-phased approach to planning, defining and beginning to operationalize an Incident Management program that is outcome-based and capability-driven. This is not meant to be a complete program framework, but outlines a high-level strategy that plots a course, and provides research-backed guidance to the first few critical steps. Effectively we set goals, define the resources necessary to achieve those goals, and provide high-level advice on achieving those goals. This three-phase approach is an aggregate of the in-depth five-step maturity model that is outlined more completely in the incident management blueprint.

Key outcomes are broken out into three components in Optiv's incident management model:

- Planning
- Coordination and execution
- Governance and measurement

These key outcomes are meant to help define the purpose of each maturity phase and give research-based insight of expected outcomes.



Phase One – Alert

Key Outcomes

- **Planning –** the first goal of developing an incident management program is to develop a cyber security incident response plan. Security teams start with defining high-level program scope, identifying key stakeholders and inventorying existing policies and processes related to remediation.
- **Coordination and Execution –** as part of the IR plan, a simple triage and verification process must be defined. It is also critical to identify security-specific incident prioritization levels (these will likely differ from IT's definitions). To support this, security teams must also establish an initial communication plan with escalation thresholds and levels of authority to act.
- **Governance and Measurement –** at this early stage, executives become aware of risks to business posed by cyber security-related incidents. Optiv recommends that the security organization take the lead in initiating a review of company policies around IT security. It is also a good time to review corporate cyber risk insurance policies (if in place).

Components

- **People**
  - Security operations personnel elevated to lead IR efforts as part time resource. Technical experts assembled in unstructured fashion to address incidents.
  - Vendor "retainer" support can provide experience in developing program requirements and identifying process gaps.
  - Legal personnel designated (part time).
- **Process**
  - Discovery and review of relevant company policies.
  - Identification of regulatory and/or insurance requirements.
  - Review industry-standard frameworks (NIST, MITRE and others) for leading practices and potential adoption.

- **Tools**
  - Perimeter and signature-based tools, implemented and managed.
  - Logging on perimeter tools must be turned on to capture logs for forensic analysts.

Capabilities

- **Verify –** establish a working definition of a cyber security incident and initial incident prioritizations.
- **Collect and Investigate –** document the existing processes for manual log collection and analysis.
- **Orchestrate –** begin program awareness effort to establish touch points with IT and helpdesk personnel.
- **Remediate –** work with IT to understand current technical remediation processes and policies.
- **Strategy –** activities out of scope at this stage.
- **Governance and Measurement -** establish a program charter with key stakeholder groups identified.
- **Preparedness –** begin consolidating process documentation into an initial incident response plan.
- **Reporting –** work with legal to understand evidence capture requirements.

Operational Advice

- Construct effective messaging to executive leadership and stakeholders. Focus on tying cyber security risks to recognized categories.
- As an industry-leading practice, start with business continuity program (BCP) definitions of critical business processes, data types and applications.
- Engage with legal early in the process of program development.
- Establishing relationships with an expert third party can help to mature the enterprise's IR program more rapidly than relying on internal resources alone.
- Investigate whether the organization has invested in cyber risk insurance. Understanding the requirements of the policy (if in place) will aid in development of a compliant response plan.

Investigate whether the organization has invested in cyber risk insurance. Understanding the requirements of the policy (if in place) will aid in development of a compliant response plan.

Phase Two – React

Key Outcomes

- **Planning –** In the next phase, the program shifts from initial stop-gap measures to adapting response plans and incident prioritizations to a generic controls framework.
- **Coordination and Execution –** Cyber incident response becomes an area of focus for Security teams, and moves out of the IT and helpdesk domains. This necessitates investment in full time security response personnel as well as establishing a formal relationship with a third-party vendor for response services.
- **Governance and Measurement –** An enterprise risk assessment effort is initiated. Relationships with legal, corporate risk, HR, audit, finance and others begin to formalize.

Components

- **People**
  - Technical response team identified. Resources are borrowed from IT functions to address incidents.
  - Some training is made available to help internal technical teams become more effective.
  - Some vendor MSAs negotiated in advance for on-call response services – to enhance response capabilities and fill skills gaps.
- **Process**
  - Processes and "incident" definitions based on generic controls frameworks.
  - A high-level cyber-security IR plan exists, but IR procedures, tools and reports are unstructured, manual and widely-vary between technical responders.
  - Security IR plan is still largely IT and security-focused, with limited and unstructured engagement from other parts of the business.

- **Tools**
  - Security leaders investigate detection technology platforms. Initial investment is made in forensics tools for case management.
  - Investment in point solutions to protect against certain types of attacks.
  - SIEM implementation mostly used for log storage. The ability to feed all technologies into SIEM requires additional investment.

Capabilities

- **Verify –** focus on tuning foundational technologies (SIEM, IPS) to be more effective for investigations and threat detection.
- **Collect and Investigate –** initialize creation of an incident response toolkit for response personnel.
- **Orchestrate –** implement processes to coordinate and track incidents.
- **Remediate –** establish protocols for IT-based remediation efforts based on incident prioritization.
- **Strategy –** prevention-focused security strategy shifts to include initial investment in detection tools and full-time response personnel.
- **Governance and Measurement -** establish basic metrics reporting to leadership.
- **Preparedness –** begin initial review and test of incident response plan.
- **Reporting –** work with legal to understand regulatory reporting requirements and criterion.

Operational Advice

- Identify points of contact with stakeholder groups (e.g., ERM, marketing communications, accounting, HR and others) for response efforts as well as "rules of engagement."
- Consider dedicating strategic resources to ongoing IR functions – such as an incident coordinator to coordinate activities amongst technical teams.

Security incident management services consist of more than technical resources. Look for incident response vendors who provide coaching and orchestration capabilities over and above technical acumen.

- Continue awareness campaign efforts with business managers and executive leadership to drive policy adoption, investment budget and support.
- Security incident management services consist of more than technical resources. Look for incident response vendors who provide coaching and orchestration capabilities over and above technical acumen.
- Consider SLAs for collection and storage and recall of logs when engaging with managed security service providers (MSSP). If not negotiated within the MSA, it can create acute difficulties for effective evidence collection in support of IR activities.

Phase Three – Respond

Key Outcomes

- **Planning –** As the program matures, static response plans become more customized. At least one adaptation of the cyber incident response plan will be developed and documented: "incident with notification."
- **Coordination and Execution –** While the security organization retains ownership of response coordination and execution efforts, other parts of the business provide designated points of contact. These roles become part of the wider response team.
- **Governance and Measurement –** Reporting (although still non-standard) goes beyond security leaders to business stakeholders. Incident definitions and priority are agreed upon by the larger business risk owners.

Components

- **People**
  - › Defined cyber security incident response team (CSIRT) is formed with standardized roles.
  - › Designated incident commander (incident management coordinator) for technical team coordination.
  - › C-level engagement.

- **Process**
  - › "Incident" definitions and prioritization customized and refined based on critical business process, asset and data classifications.
  - › Identified roles and responsibilities. Program framework develops initial high-level RACI (Matrix of stakeholders, categorized as: Responsible, Accountable, Consulted or Informed).
  - › IR plan variation is identified: Incidents vs Incidents with notification. "Triggers" and rules of engagement established and documented for extended team.
- **Tools**
  - › Incident management tools investment. Standard response toolkits to provide some automation of collection, investigation and analysis efforts.
  - › Forensics tools with agents deployed to support volatile data collection.
  - › Network-monitoring and detection tools provide automated event correlation, application analysis and sandboxing.

Capabilities

- **Verify –** focus on enhancing detection capabilities.
- **Collect and Investigate –** tool-supported processes used for data collection, aggregation and analysis.
- **Orchestrate –** lessons learned captured and documented for planning purposes.
- **Remediate –** response teams begin to perform root-cause analysis on high priority incidents.
- **Strategy –** response efforts become cyclical, everyday activities; investment in response capabilities become a major component of security strategy.
- **Governance and Measurement –** reporting to executive-level. Lessons learned support data-driven decision-making.
- **Preparedness –** standard timelines for testing and review of incident response plans. Training for response team becomes a priority.
- **Reporting –** compliance and regulatory reporting efforts are performed on case-by-case basis, led by legal.

Operational Advice

- Completing the risk assessment will lead to a better understanding of critical business processes, data assets and applications.
- Clearly defining roles and responsibilities along with appropriate documentation is important for repeatability and standardization as well as identifying remaining gaps in the program.
- If resources dedicated to a response team are not possible, consider investing in an incident response platform. This technology allows for "build once, run many" and can help coordinate and prepare part-time response resources.
- Consider engaging a third party for red team / blue team reviews. Performance during these reviews can help identify gaps in response team training and overall program capabilities.
- Continue looking for interconnects between cyber security IR plans and disaster recovery (DR), crisis management and/or other business continuity plans (BCP). Consider how to initiate a DR or crisis management scenario in case a crisis-level cyber incident was to occur.

The three phases outlined above correlate to the first three levels of maturity on the overall program scale. Achieving these first three levels provides for a way to plan and execute the program strategy in manageable components, with key milestones and deliverables designed to demonstrate progress towards the overall business objectives.

Call to Action

The ever-evolving threat landscape and rising cost of data breaches demands stronger and broader preparation for effective security incident management and response. Adopting a program strategy approach to managing cyber security incidents requires a structured, well-orchestrated response.

Program strategy starts with a clear definition of roles and responsibilities across the enterprise. A business-aligned program must involve key stakeholders from business critical functions such as legal, enterprise risk, IT and others in order to be successful. By defining key performance indicators (KPIs) based on risk instead of IT-focused metrics, the program rises to the level of enterprise priority.

Security incident response and security incident management programs provide significant value to the business. These programs support planning and testing a proactive IR plan. These programs also provide an opportunity to elevate perception of the CISO and the security organization to that of business enabler. A current, tested business-aligned incident management program supports a more resilient business.

References:

1 – The Cyberbuck Stops Here!, Sabbatt,R.V., ISSA.
https://c.ymcdn.com/sites/www.issa.org/resource/resmgr/journalpdfs/feature0115.pdf

2 – Cost of Breach Report, Ponemon and IBM.
http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03053WWEN&attachment=SEW03053WWEN.PDF

1125 17th Street, Suite 1700
Denver, CO 80202
800.574.0896
www.optiv.com

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.

2.16 | F1V2