Incident Response: How to Fight Back

A SANS Survey

Written by Alissa Torres

Advisor: Jacob Williams

August 2014

Sponsored by

Bit9 + Carbon Black

Executive Summary

Highly public breaches at companies such as Target, Evernote and Living Social, which collectively compromised more than 200 million customer records, are pushing many organizations to develop in-house incident response (IR) capabilities to prevent such data breaches.

Key Results

- Many IR professionals feel their organizations' IR capabilities are ineffective.
- Broad definitions of an *incident* place a strain on IR teams.
- Lack of time to review and practice IR procedures is a primary barrier to effective IR.
- Lack of formalized IR plans and dedicated staff plague most organizations.
- Organizations need to implement collection and correlation of threat intelligence.
- Security information and event management (SIEM) tools are the focus for those working to improve their IR capabilities.

IR teams, typically operating under a formalized IR plan, are designed to detect, investigate and, when necessary, remediate organizational assets in the event of a critical incident. SANS conducted a survey focused on the current state of IR during May and June 2014, polling security professionals from more than 19 industries and various-sized companies and organizations. The goal was to get a clearer picture of what IR teams are up against today—the types of attacks they see and what defenses they have in place to detect and respond to these threats. In addition, the survey measured the IR teams' perceived effectiveness and obstacles to incident handling.

Of the 259 survey respondents, 88% work in an IR role, making this a target audience for soliciting close to real-time data on the current state of IR. Respondents represented 13 different regions and countries and work in management (28%), or as security analysts (29%), incident responders (13%) and forensic examiners (7%). This broad representation helps shed light on both present and future IR capabilities.

Some of the key findings from the report include the following:

- **More than one-quarter of IR professionals (26%) are dissatisfied with their current organization's IR capabilities, calling them *ineffective*.** Only 9% categorize their processes as *very effective*. Notable impediments to IR include lack of time to review and practice procedures (62%) and lack of budget for tools and technologies (60%).
- **The definition of an incident remains broad, increasing the workload for already understaffed IR teams.** The breadth of incident types is immense and not limited solely to network breaches and malicious software. IR teams are often tasked with handling unauthorized accesses from external and internal sources, distributed denial of service (DDoS), insider misuse and data loss.
- **Efficient response to security incidents is hindered by lack of time to review and practice IR procedures.** The most cited obstacle to effective IR processes was lack of time to practice response procedures (62%), speaking to the need for both hands-on walk-throughs and mock exercises that test written policies and aid in standardizing triage and response in enterprise incidents.

- **Lack of formal IR response plans and defined team structures were identified as detriments to efficient incident handling.** Lack of formal IR plans and procedures present obstacles to 43% of respondents. Fifty-five percent of respondents identified the lack of a formal IR team as an obstacle to effective response. The majority (61%) draw in additional assistance from their internal IT staff to address their IR surge needs.
- **Organizations have not yet implemented the collection and correlation of threat intelligence.** Only 31% of respondents are attempting to perform attacker attribution as part of their analysis of incidents affecting their organizations, crippling their capability to detect the same adversary upon his or her next targeted campaign.
- **Automation and SIEM integration tools remain the focus to improve IR processes.** Projected improvements in IR capabilities focus on increasing analysis and reporting capabilities through automation and expanding SIEM integration, selected by 68% of respondents. Tools that increase visibility into threats and how they apply to their environment, including scoping and remediation capabilities, are where teams are spending their budgets.

This report includes these and other findings.

About the Survey Respondents

A total of 19 industries are represented in the survey. Of the 259 respondents, 15% are from the technology/IT sector and 14% are from the financial services industry. Education and health care/pharmaceuticals are each represented by at least 8% of respondents, as illustrated in Figure 1.

What is your company's primary industry?

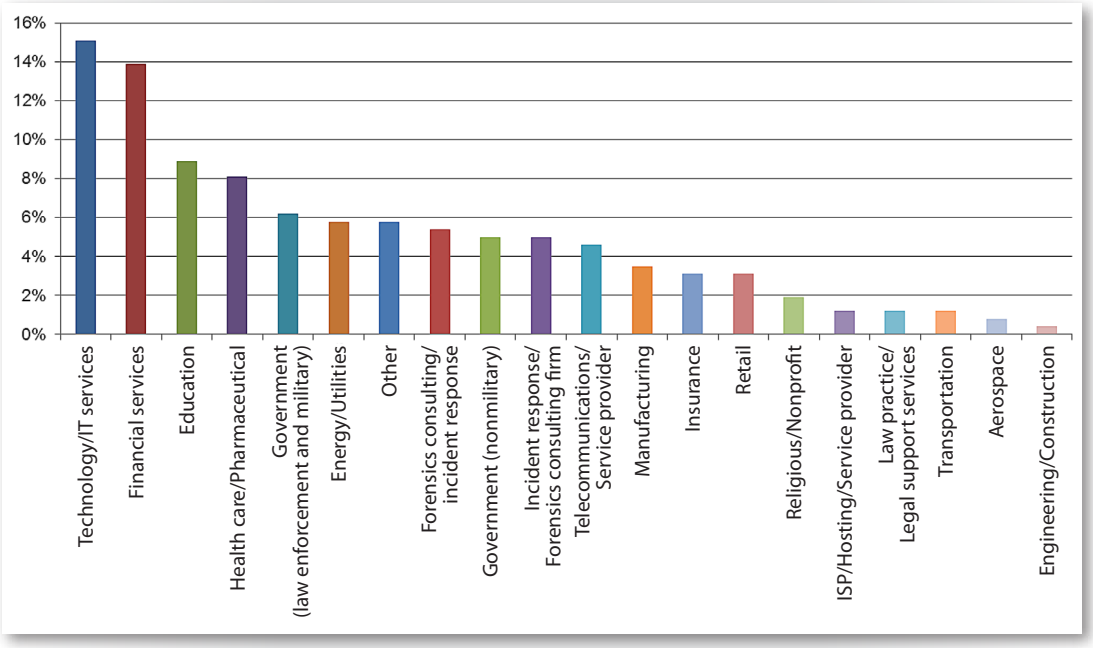


Figure 1. Industries Represented

Respondents represented 13 regions and countries, with many from companies having a global presence. Most (72%) work for companies that have a presence in the United States (see Figure 2).

In what countries or regions does your organization perform incident response activities? *Select all that apply.*

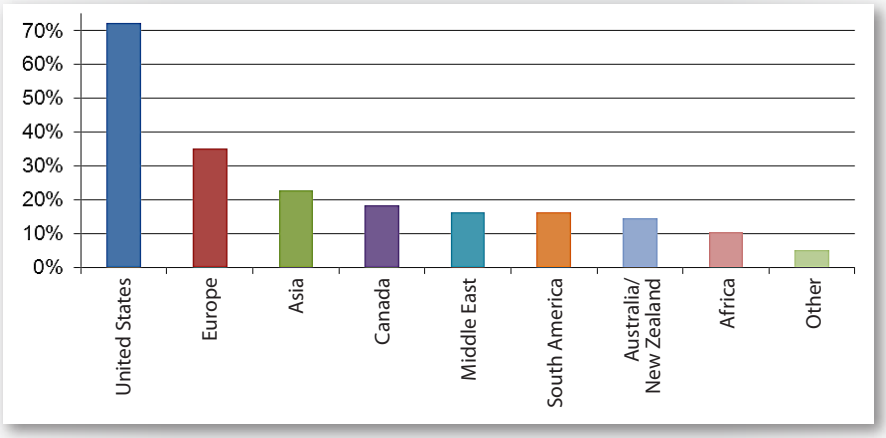


Figure 2. Countries and Regions Represented

Most respondents (88%) are involved in their organization's IR process. To this point, 33% have led the remediation of incidents, 23% have assisted in detection, 20% have assisted in remediation efforts and 12% have participated in discovery or reporting of incidents. Figure 3 illustrates the roles respondents played in the IR process.

Did you play a role in any of the above incidents' detection, analysis or remediation? If so, what was that role?
Please select the most appropriate answer.

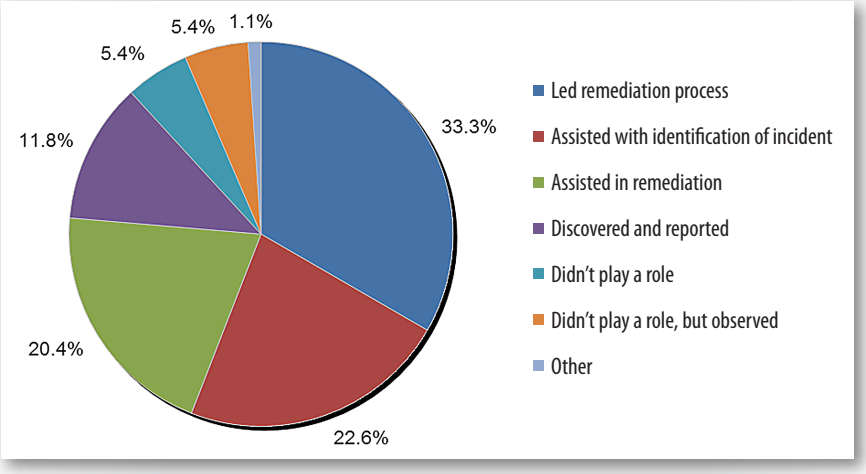
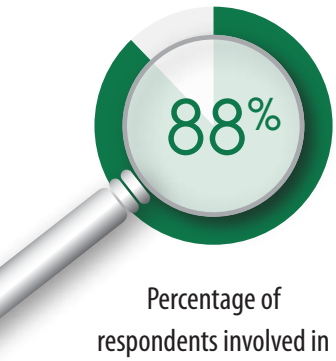


Figure 3. Participant Roles in Incident Handling



Percentage of respondents involved in the IR process

Input came from professionals of varying roles. Security analysts (29%) made up the greatest portion of participants. However, forensic examiners (7%) and incident responders (13%) were well represented, as were supervisory roles (28%), including security manager/director/CISO/CSO or IT manager/director/CIO, as illustrated in Figure 4.

What is your primary role in the organization, regardless of whether you are considered an employee or consultant?

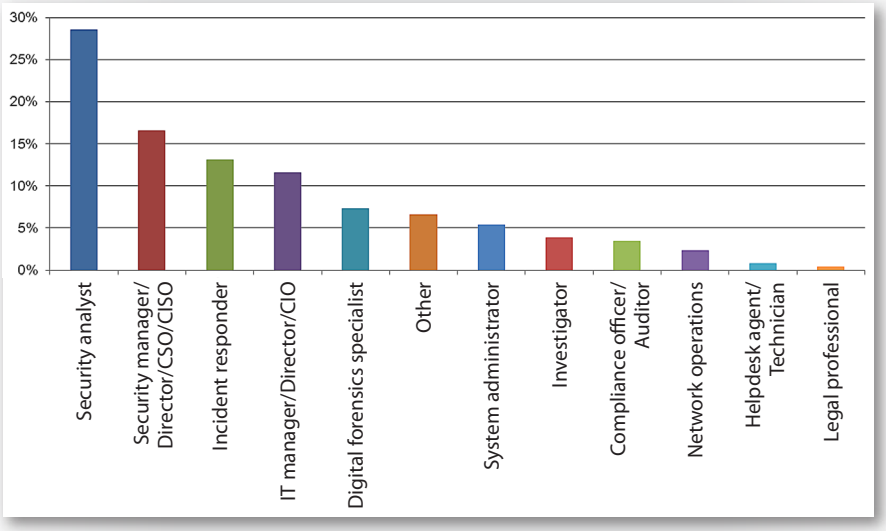


Figure 4. Organizational Roles

Given that all survey respondents stated they work in an IR role, this illustrates the wide range of skills required to successfully tackle an incident. Organizations should look to increase both breadth and depth in their IR teams.

Representation was strong from large companies of more than 20,000 employees (24%) and smaller companies with fewer than 100 employees (17%). Figure 5 illustrates the balanced representation from varied sizes of organizations.

No matter the size of the company, organizations are facing incidents and require IR capabilities.

How large is your organization's workforce, including both employee and contractor staff?

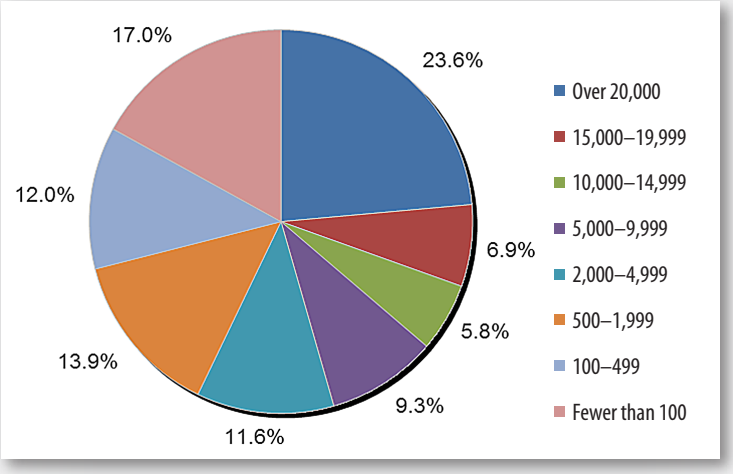


Figure 5. Organizational Size

So, no matter the size of the company (large or small), organizations are facing incidents and require IR capabilities.

Taking all of the demographic results together, the survey sample provides a good cross-section of those working in security with an emphasis on IR at all levels.

Incidents Happen

Incidents are becoming more commonplace. Although 21% of respondents didn't know if their organization had experienced an incident, 61% reported experiencing at least one incident involving a data breach, unauthorized access, denial of service or malware infection over the past two years. The largest percentage of respondents (48%) experienced up to 25 incidents, as illustrated in Figure 6.

Over the past two years, how many critical incidents (such as those resulting in data breach, unauthorized access, denial of service) has your organization experienced that required incident response?

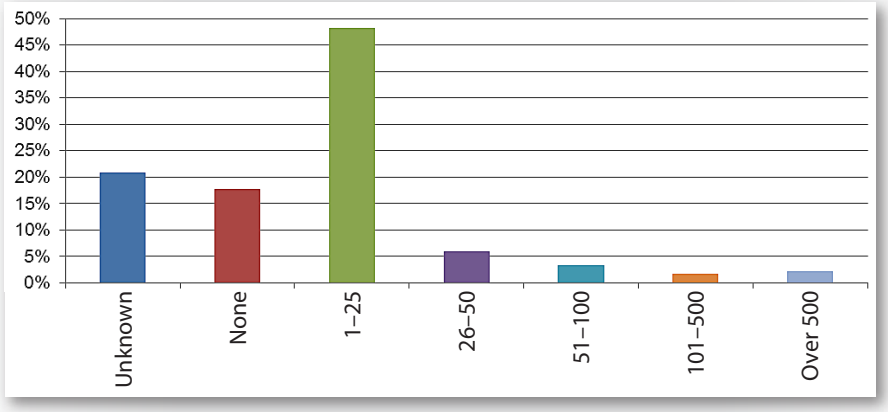
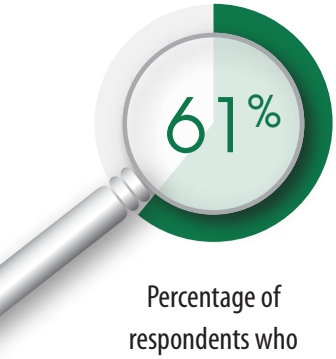


Figure 6. Critical Incidents in the Past Two Years



Percentage of respondents who experienced at least one critical incident in the past two years

Organizational size seems to have little effect on the prevalence of experiencing an incident. The same percentage of respondents from organizations with fewer than 100 employees (61%) reported at least one incident, as did the entire sample. This data continues to refute the perception that being a smaller target offers protection against information security incidents. Figure 7 provides a snapshot of such organizations' experience with incidents.

Over the past two years, how many critical incidents (such as those resulting in data breach, unauthorized access, denial of service) has your organization experienced that required incident response?

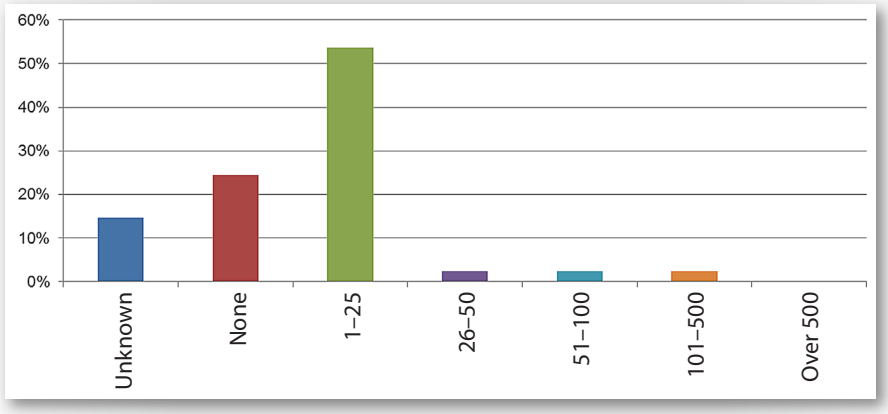
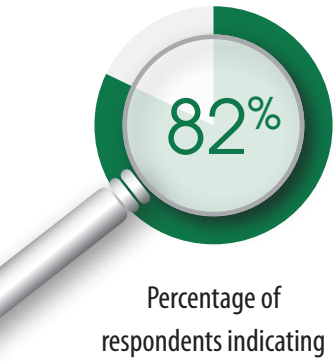


Figure 7. Critical Incidents for Companies with Fewer Than 100 Employees

Due to widely varying definitions of the term *incident*, respondents reporting more than 100 security incidents (4%) may be experiencing "scope creep" and use a wider definition of *incident*, thus increasing the different types of events that fall to IR teams to investigate. These may include additional situations such as equipment loss/theft, employee misuse and data leak.

Incident Type

Although many respondents might have experienced equipment loss or other situations, it is no surprise that the most common incident type involved malware (82%), with 18% experiencing more than 20 malware infections over the 24-month duration. The second most frequent category of incident was unauthorized access (70%). Figure 8 illustrates the type and frequency of incidents experienced by respondents.



Percentage of respondents indicating malware is their most common incident type

What was the nature of the incidents? If possible, please provide the frequency for each type of incident or false alarm experienced.

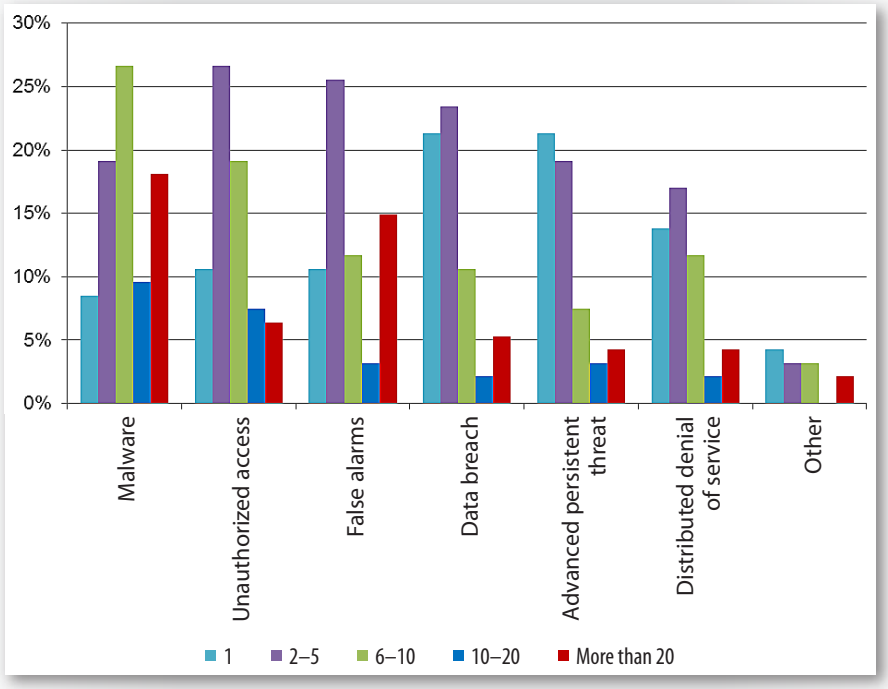


Figure 8. Nature and Frequency of Critical Incidents

Incidents involving false alarms (66%) plagued 15% of respondents who experienced more than 20 over the same time frame. Eliminating false positives is part of IR triage, but today's over-tasked IR teams can hardly afford to spend valuable cycles alerting on systems that are not compromised.

Possible techniques for reducing false alarms include performing scheduled tool and indicator baselining to optimize network sensor alerts and host-based indicators, as well as in-house training for team members to become more familiar with what *normal* looks like. As detection tools and IR staff become better attuned to the organization's unique environment, false-positive alerts will occur less frequently, optimizing detection and response time.

As detection tools and IR staff become better attuned to the organization's unique environment, false-positive alerts will occur less frequently, optimizing detection and response time.

Another technique to reduce false positives is to use event correlation capabilities with SIEM platforms to match criteria and group unique events from disparate devices and applications as a single alert. This implementation increases the reliability of the alert and decreases the possibility of "alert fatigue," which is often experienced by security analysts charged with following up on too many unsubstantiated alerts.

DDoS attacks are often associated with extortionists, hacktivists or politically motivated attackers wanting to make their agenda known. The high percentage of respondents (49%) who experienced this type of attack is consistent with the 2014 Verizon Data Breach Investigation Report, which included DoS attacks as one of its nine detailed breach patterns, making up 3% of all incidents experienced by their contributors.[1] The survey respondents were not immune by any means. Of respondents, 17% saw from 2–5 incidents, and 4% experienced more than 20.

IT personnel and management may believe that only very large organizations experience DDoS attacks;[2] however, the median size of the organizations in the survey was less than 5,000 people. These results seem to indicate that many organizations considered relatively small were also impacted by DDoS attacks. IR teams large and small should prepare for this type of attack, which is particularly easy for adversaries to carry out on a budget as small as $50.[3]

[1] www.verizonenterprise.com/DBIR/2014

[2] http://threatpost.com/google-project-shield-to-protect-sensitive-sites-from-ddos-attacks

[3] "Figuring DDoS Attack Risks Into IT Security Budgets," www.forbes.com/sites/ciocentral/2012/05/08/figuring-ddos-attack-risks-into-it-security-budgets

Impact of Data Breach Incidents

A *data breach* is defined as theft of sensitive data such as intellectual property or records containing an employee or customer's name and associated sensitive data, for example, health information or financial account information. In the 2014 Cost of Data Breach Study from Ponemon Institute, the average cost to a company suffering a data breach affecting personally identifiable information (PII) was $3.5 million, with an average cost per sensitive record of $145.[4] Organizations spend approximately 50% of the cost of being a victim of a data breach on crisis services, including forensics services, as seen in a study conducted by NetDiligence in 2013.[5]

What was the most common data attackers stole? The two top categories, each named in 36% of responses, were employee information and individual customer information. In addition, both proprietary customer information and intellectual property loss were found in 32% of respondents' data breaches (see Figure 9).

Additional consequences of customer data loss that are less easy to quantify involve damage to reputation, degraded public opinion of the company's brand and loss of market share.

If you experienced a data breach in the past two years, what type of data was exfiltrated from the environment? *Please select all that apply.*

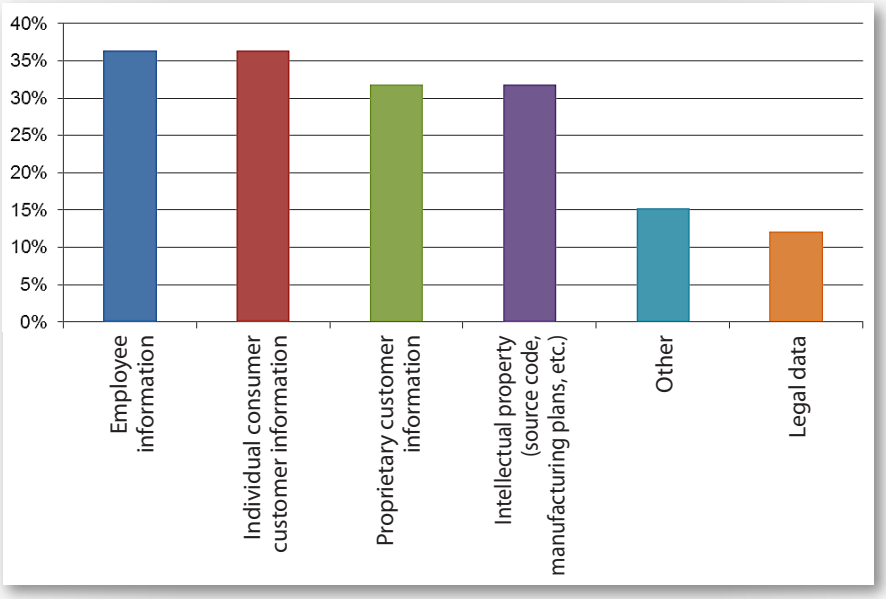


Figure 9. Type of Data Stolen in Breaches

Reporting breaches to regulators, customer notification requirements, card replacement fees and consumer credit monitoring subscription costs make the loss of customer data a very lengthy and expensive situation for companies. The Target breach in late 2013 is estimated to have cost financial institutions more than $200 million in credit card replacement fees.[6] An effective IR program detects compromises earlier in the attack life cycle, lowering the cost incurred when an organization suffers a compromise, possibly even preventing a breach from succeeding.

[4] "The cost of a data breach in 2014: $3.5 million, Ponemon study says," www.itworldcanada.com/article/the-cost-of-a-data-breach-in-2014-3-5-million-ponemon-study-says/93140

[5] "Cyber Liability & Data Breach Insurance Claims," www.netdiligence.com/files/CyberClaimsStudy-2013.pdf

[6] "Cost of Replacing Credit Cards After Target Breach Estimated at $200 Million," http://on.wsj.com/1j0muzQ

Incident Handling

Although 59% of respondents have a dedicated IR team, many respondents (27%) make use of third-party IR service providers to augment or handle incidents on an as-needed basis. In addition, 23% use an IT management provider to aid in IR. Based on the aggregate number of responses, some organizations with internal teams outsource particular incident types to third-party services and handle others on their own, as illustrated in Figure 10.

What resources does your organization utilize in responding to incidents?
Select all that apply.

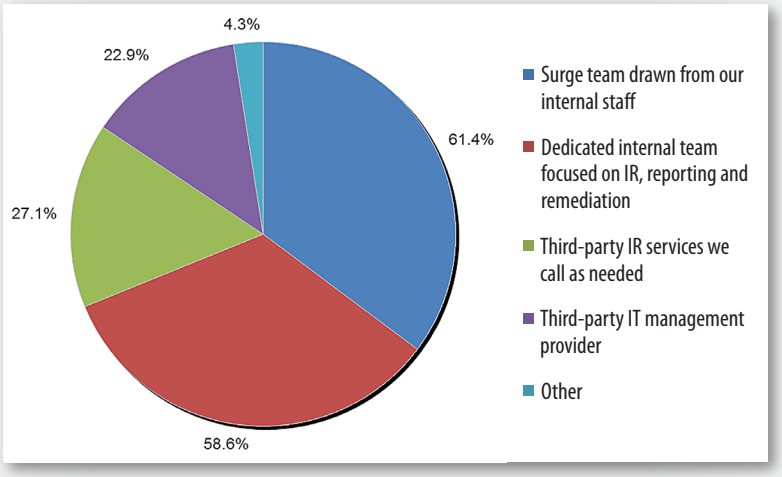


Figure 10. Types of IR Resources Utilized by Organizations

According to respondents, investigations that involved company-owned laptops, smartphones, tablets and other company-owned mobile devices were the most common (62%) incident type handled internally. In contrast, the more frequently outsourced incident types involve business applications in the cloud (18%) such as SAP, email or web applications, such as Dropbox, followed closely by in-the-cloud marketplaces using shared applications (17%).

Internal IR teams are likely to have the skills to handle incidents involving only commodity assets, such as laptops and mobile devices. However, few IR professionals have the skills to investigate an incident involving SAP or AS/400 (both very common in business today). Incidents involving these assets usually require the help of an outside specialist. Additionally, there is a natural gap between the availability of tools to investigate commodity assets and such specialized technologies, furthering the need to augment internal staff with outside experts.

Incident Response Effectiveness

The survey data shows that organizations are experiencing a wide range of incident types with varying degrees of frequency, and they are using a variety of resources. But how effective are their efforts?

Only 9% of respondents were happy with their IR capabilities, including their outsourced processes. Almost 26% thought their capabilities and processes to be ineffective, as illustrated in Figure 11.

The rate of increasing complexity in today's malware and attacker techniques is not slowing, and if an organization's IR capabilities are behind the curve now, that trend is likely to continue.

How effective do you feel your incident response capabilities and processes are (including your outsourcing arrangement, if applicable)?

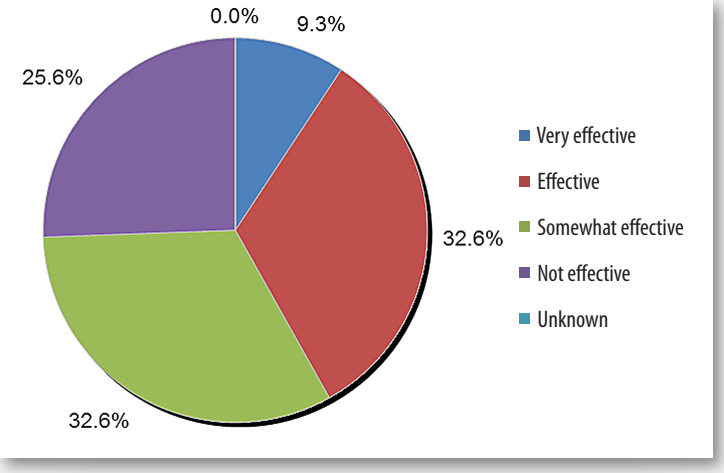


Figure 11. Effectiveness of IR Capabilities and Processes

So, although 42% of respondents feel they are adequately prepared to handle incidents, the remaining 58% need to improve their capabilities. As the race between sophisticated attackers and watchful defenders ensues, the percentage of IR professionals who feel their capabilities are in need of improvement is not likely to change. The rate of increasing complexity in today's malware and attacker techniques is not slowing, and if an organization's IR capabilities are behind the curve now, that trend is likely to continue.

The best way to break down the survey results is to focus on the six steps of IR and how respondents felt their current structure and capabilities provided successful completion of each step.

Six Steps of Incident Response

1. Preparation
2. Identification and scoping
3. Containment
4. Eradication
5. Recovery
6. Lessons learned

Importance of Preparation

A huge part of the preparation stage of an organization's IR capabilities is defining roles and responsibilities, creating buy-in and garnering support from upper management and data-owning business units. Without moving through a collaborative process of creating a formal IR plan and procedures, as 43% of respondents have not yet done, those working in the IR role are often left to figure out procedures and sidestep political landmines during times of crisis. But the Ponemon Institute found in its 2014 Cost of the Data Breach report that organizations that suffered a data breach and maintained an IR plan lowered the cost per sensitive record lost by up to $12.77.[7]

A secondary benefit to formalizing an organization's IR plans through collaborative efforts prevents barriers to communication that occur when IR goals are not fully aligned with service level agreements (SLAs) and business continuity. Respondents noted that silos existing between IR and other business units (36%) and HR/legal impediments to investigation/monitoring (14%) act as obstacles, further confirming the detriments to a lack of formalized process for working IR investigations (see Figure 12).

What do you believe are the key impediments to effective IR at your organization?

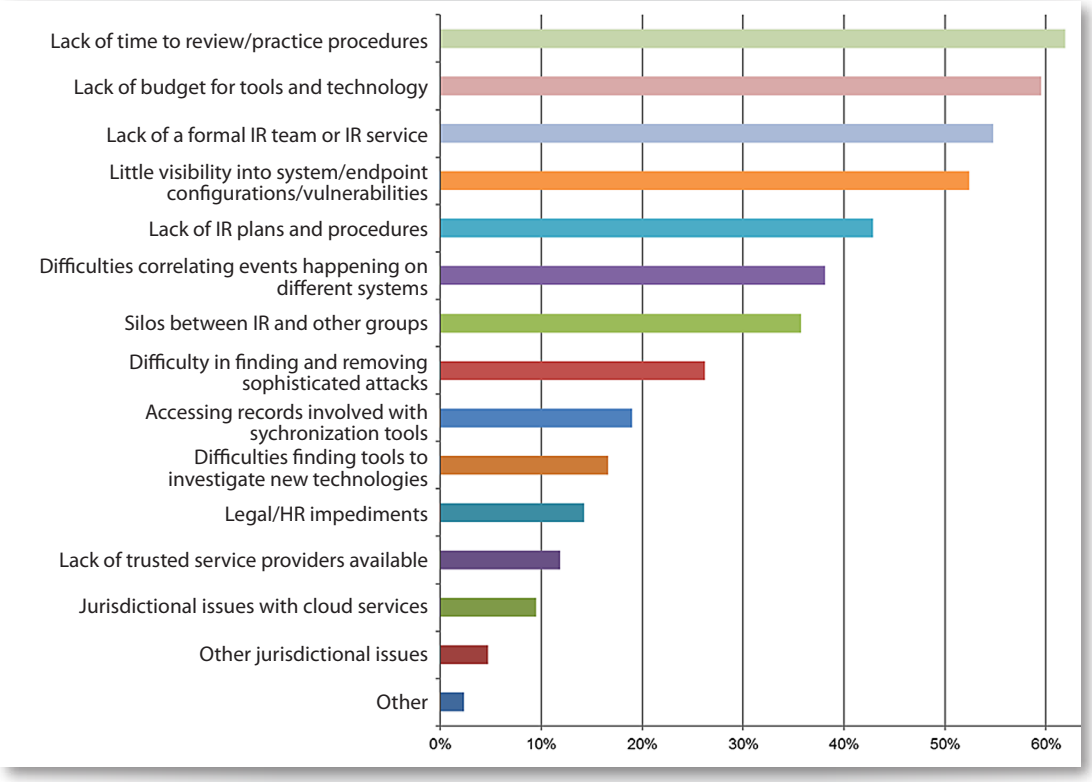


Figure 12. Impediments to Effective IR

[7] "The cost of a data breach in 2014: $3.5 million, Ponemon study says," www.itworldcanada.com/article/the-cost-of-a-data-breach-in-2014-3-5-million-ponemon-study-says/93140

Another key part of the preparation phase is IR team staffing. The majority of respondents (55%) cited the lack of a formal IR team with dedicated members as an obstacle to effective IR. Many organizations lack the necessary funding to staff a fully dedicated team whose sole focus is on detecting and responding to an incident.

In some environments, the role may fall to a sole individual, who is assisted by "surge staff" during the investigation of a serious incident. Obvious pitfalls to this team structure include a lower likelihood of recognizing a serious incident due to a lack of analysis resources and adding untrained workers pressed into service at times of high criticality and high visibility, such as after a breach becomes publicly known. Not only do inexperienced staff not have proper triage and investigative skills, but they also require a great deal of oversight and guidance, taking the lead IR staffer away from managing the work and acting as a liaison to upper management and other business units.

Percentage of respondents citing lack of a formal IR team with dedicated members as an obstacle to effective IR

There is no ideal team structure that will work for every organization because complexity of network infrastructures and number of endpoints varies widely. Yet, for effective response management to exist, someone must be held accountable for its oversight, care and feeding. Without explicitly assigned accountability, implementing an effective IR process and procedures can be pushed aside as an ancillary duty.

A third aspect of IR capability preparation includes proactively deploying security tools tailored for IR on the endpoints prior to a breach. A majority (52%) of respondents cited lack of visibility into system/endpoint vulnerabilities as an obstacle to efficient IR. This highlights a common problem: Many organizations put security tools in place as a reaction to a breach instead of in preparation for one. Such tools allow for real-time and continuous monitoring of company endpoints, and if done in the preparation phase—prior to an incident—endpoint sensors can provide a full audit trail to aid in understanding an attack and properly scoping the environment with real-time and historic data.

Methods of Detection

After preparing for the inevitable endpoint compromise, *detection* of a compromise is the next most important step. In fact, none of the other steps in the process can occur without detection. But given the workload of the average security analyst, automation is an important component of detection. SANS asked survey participants which techniques they use to detect suspected compromises and whether these techniques are automated. Figure 13 illustrates their responses.

Given the workload of the average security analyst, automation is an important component of detection.

How does your organization identify impacted systems, and how automated are these processes of identification?

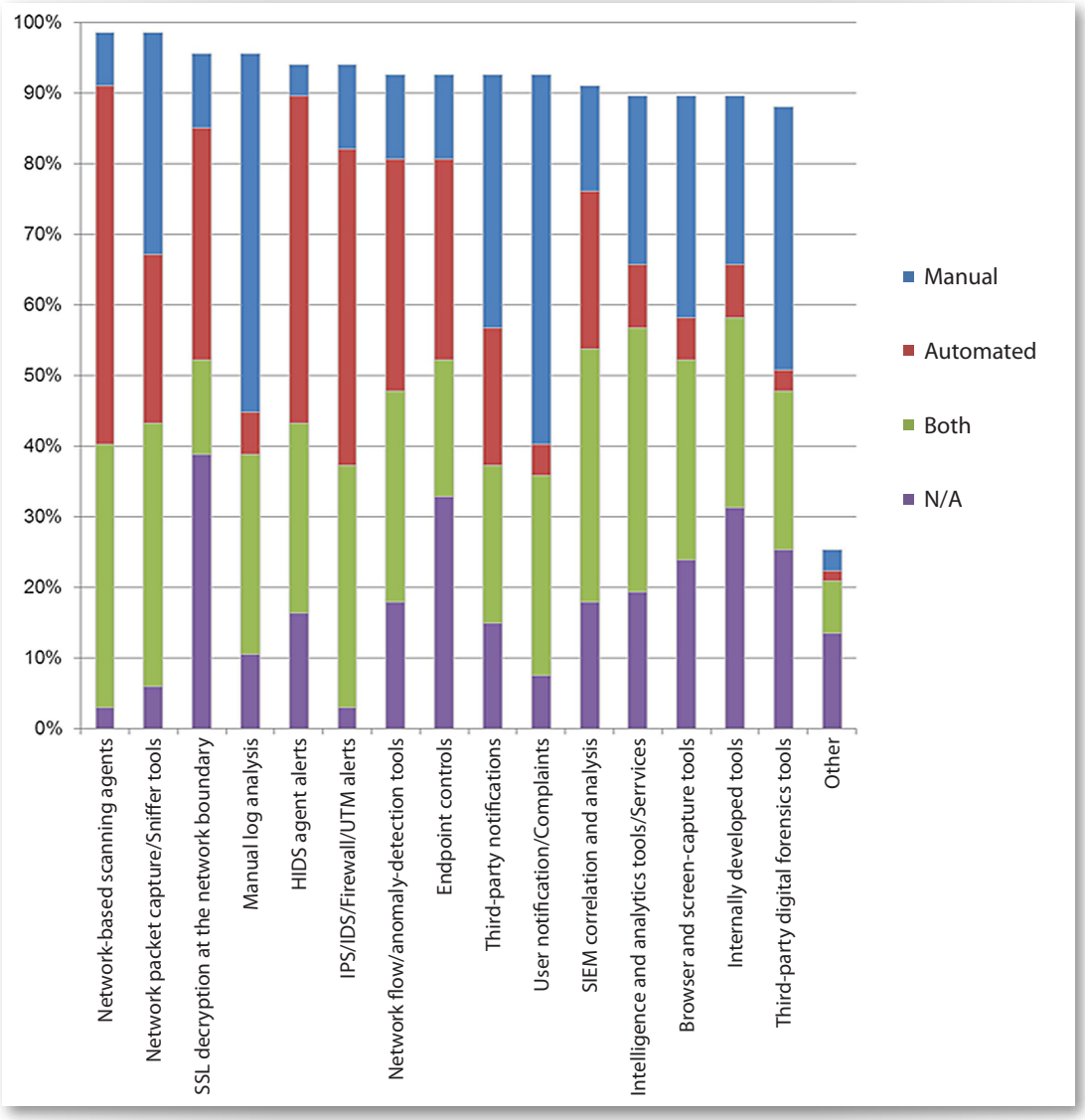


Figure 13. Detection Methods

The three most popular techniques (each used by more than 90% of the participants) are scanning for indicators with agents (96%), analyzing network capture (93%) and responding to firewall, IPS/IDS or UTM alerts (91%).

Participants reported high levels of automation for agent-based scanning and firewall/IPS/IDS/UTM alerts, but the second highest level of automation reported was detection using host-based intrusion detection (HIDS) agents. Participants also reported high levels of automation with HIDS agents (46%, second highest in the survey overall), but a full 16% do not use HIDS at all. This lowers HIDS popularity for detection to sixth overall. The top 5 are listed in Table 1.

Table 1. Most Popular Detection Tools

Technology	Percent Using
Network-based scanning for indicators with agents	96%
Analyzing network capture	93%
Responding to firewall, IPS/IDS or UTM alerts	91%
User notification or complaints	85%
Manual log analysis	85%

Perhaps just as interesting is what participants are *not* using for detection. The three least used technologies in the survey are SSL decryption at the network boundary (39% do not use), endpoint controls such as network access control (NAC) or mobile device management (MDM) (33% do not use) and homegrown tools tailored to the environment (31% do not use).

The low adoption of NAC, MDM and SSL decryption may indicate that tool maturity (or perceived maturity) and the ease in which these functions can be implemented as detection mechanisms have a ways to go. Though not currently used by a good portion of respondents, the usefulness of these technologies as preventive controls is undeniable. For example, as endpoint devices travel between home and various worksites, connecting to public hotspots and unprotected home networks and increasing the chances of malware infection, implementations such as NAC ensure a device is scanned and deemed healthy prior to allowing it access to internal network resources.

The fact that commercially available tools are meeting participants' needs may explain the limited use of homegrown tools in place of SIEMs. Alternatively, participants may lack the expertise in-house to design, build and maintain such tools.

One additional finding worthy of mention is that 18% of participants do not use a SIEM at all, while 85% still perform some type of manual log analysis for the *identification* of incidents. It is unclear whether this is due to lack of training, system availability or some other factor. SIEM providers should perform further research to determine the reasons why manual log analysis has a higher overall adoption rate than the use of a SIEM and why some percentage of SIEM users still rely on manual log analysis for the identification of incidents.

Teams without the ability to classify and qualify alerts—functions a SIEM typically provides—may be unable to properly prioritize and may perceive every alert as critical, quickly overwhelming a small team's resources. For respondents who implement a SIEM and are still conducting manual log review, factors such as a SIEM's limited visibility into certain areas of an organization's network or decreased granularity due to high-level filtering of data aggregates may be likely reasons for this continued analysis requirement.

Containment

One measure of IR team maturity is how rapidly the team can move an incident from initial detection to *containment*, which means isolating affected systems to stop additional infections and prevent additional data theft. One of the most important IR goals is to keep loss and the impact to the organization down to acceptable levels.

It is this time frame that is critical in many instances in mitigating the severity of loss. The most common time frame from discovery to containment and implementing virtual or physical isolation of affected systems, chosen by 19% of respondents, was 4–8 hours. The second largest group of respondents (16%) called out the 1–4 hour time frame. Only slightly fewer (14%), however, required 2–7 days for containment. Obviously, the smaller the window of time the better (see Figure 14).

From the time the incident was discovered, how much time elapsed until containment was accomplished?

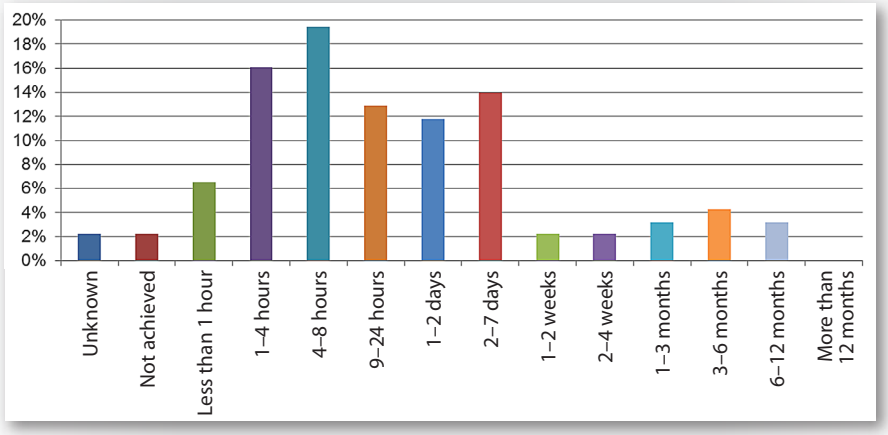


Figure 14. Elapsed Time from Discovery to Containment

What obstacles are impeding a team's ability to contain the system immediately? After receiving an alert based on network- or host-based indicators, an IR team must perform triage on the system(s) to properly confirm a security incident. In most sprawling global enterprises today, responders make remote connections in order to ascertain the system state of the alerted system.

Remote forensics/IR tools effectively decrease triage data collection time, allowing teams to speed system containment by valuable minutes or even hours. If an IR team does not have remote forensic/IR agents on the endpoint systems, other system survey scripts might be run remotely or an IT or security technician on site might be tasked with performing the triage locally. More recently, some enterprise IR tools have added features that can automate alert confirmation, isolation, analysis and incident resolution to achieve rapid-response capabilities, thereby freeing up valuable security analyst and IR human resources. These alternatives aid in reducing the time from detection to containment.

Remote forensics/ IR tools effectively decrease triage data collection time, allowing teams to speed system containment by valuable minutes or even hours.

In many network intrusion cases involving sophisticated attackers, initial system triage of potentially compromised systems sets off a race between the investigating team and the attacker. Because responders run collection/triage tools on systems that deviate from normal activity, the chance of tipping off an attacker that detection has occurred is of particular consequence. Expected attacker actions, once they suspect detection, include minimizing their footprint on the network by wiping malicious files and toolsets from compromised systems or changing their behaviors to avoid further detection. Clearly, the less time an IR team gives the attacker to react after detection, in most cases, the better.

A large percentage of respondents had longer time frames in moving to containment—15% reported periods of longer than 7 days, and 11% reported taking a month or longer. Some of these organizations may have elected not to immediately contain affected systems but, instead, monitor attacker activity in order to gather threat intelligence and aid in attacker attribution. By completing attribution of an attacker, the IR team is better able to understand the threat and gains valuable indicators of compromise (IOCs) that they can use to detect future attacks that would otherwise have flown under the radar.

Remediation and Recovery

Successful remediation involves eradicating the malicious actor from the network and returning to business as usual: getting systems back online and restoring availability of affected services to internal and external customers.

In many critical incidents, there are potential financial implications for every minute an organization's network or system services are degraded, whether the system is a web server that had to be taken offline or an employee's workstation that required a complete rebuild.

Based on this, an important IR performance metric is the time it takes an organization to move from detection of a critical incident to full remediation. The most common survey response (22%) is a 2–7 day window from detection to remediation, as shown in Figure 15.

Percentage of respondents identifying improved remediation processes as an area for improvement

From the time the incident was discovered, how much time elapsed until remediation was achieved?

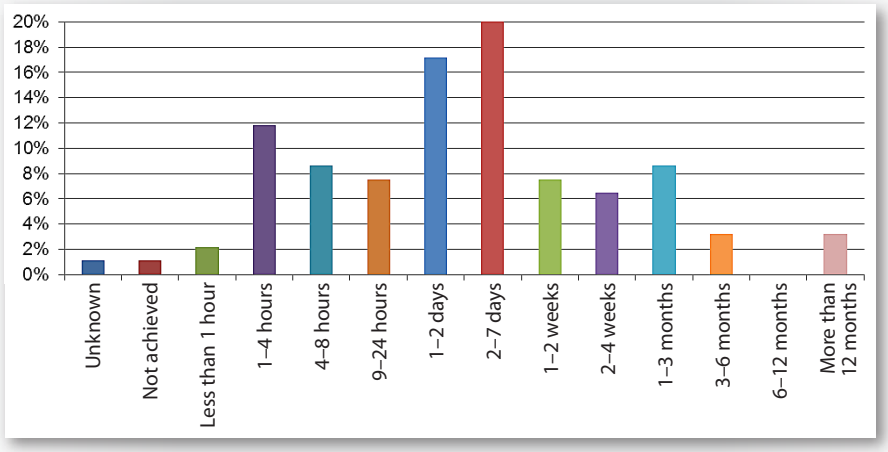


Figure 15. Time from Discovery to Remediation

Additionally, 29% of respondents reported taking over a week to remediate the incident, and 4% took longer than 12 months or never remediated the issue. What hurdles are slowing these organizations' IR processes, requiring them to experience notable delays? And are these time frames acceptable? As later survey questions reveal, 54% of respondents named improved remediation processes as an identified area of improvement over the next two years, supporting the idea that current time frames from detection to remediation are unacceptable.

Part of IR preparation is working with upper-level management to define an *acceptable interruption window (AIW)*, the time an incident can continue before the interruption the incident causes starts to become unacceptably adverse in terms of its consequences. With 15% of respondents citing a detection to remediation period of one month or more, an excellent follow-up question might be to determine whether these organizations have calculated an AIW and whether the impact of these critical incidents fell within their acceptable limits. Regardless, organizations of all sizes should look to establish an AIW based on their business models.

Impediments to remediation include lack of well-developed IR processes, shortage of in-house or readily available forensics/IR investigators and limited access to threat-specific remediation advice. Organizations without these resources have difficulty determining proper scoping for an intrusion and typically are unable to do the following:

- Analyze their initial system to identify signature malware and attacker behaviors and generate indicators of compromise
- Properly scan and identify other compromised endpoints on the network involved in the intrusion
- Effectively broaden the scope to include endpoints without active malware based on trace system artifacts and use of previously compromised accounts
- Reduce the potential damage by disabling specific applications or services that are the means for compromise and/or data exfiltration

Perhaps one of the lessons survey participants learned through their experiences is the need for more automation and integration with SIEM technology. When asked about the areas of their organizations' IR process they planned to improve upon over the next 24 months, a full 68% of participants indicated they plan more integration with the SIEM. Improved visibility into threats and vulnerabilities was the second most frequent improvement, cited by 59% of respondents (see Figure 16).

What improvements is your organization planning for incident response programs over the next 24 months? ***Select all that apply.***

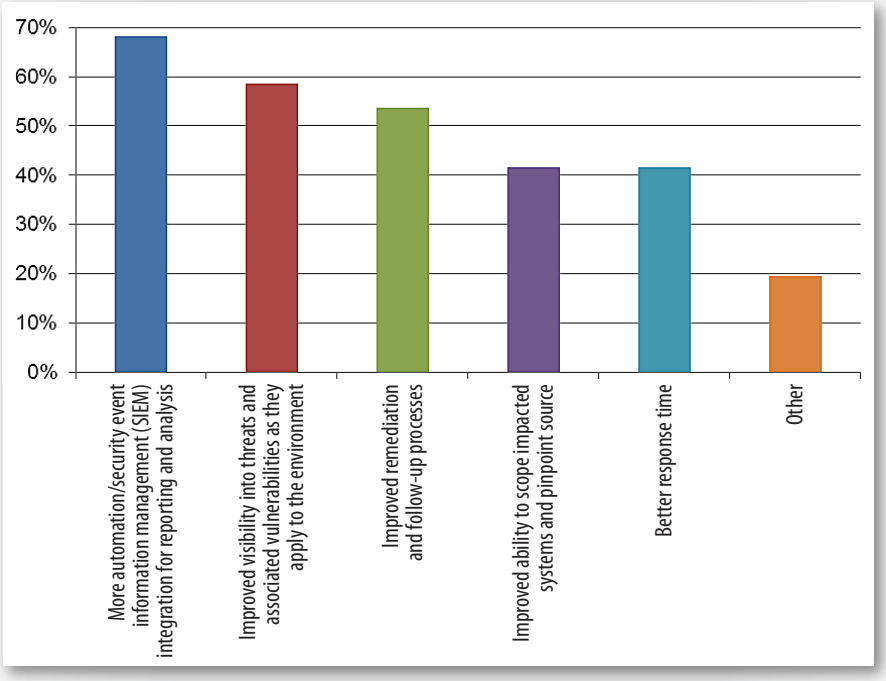


Figure 16. Planned Improvements

Both improved integration of the SIEM and improved visibility focus on faster and more efficient detection of anomalous behaviors. The 2014 Verizon Data Breach Investigations Report (DBIR),[8] supports these self-identified weaknesses in security teams today. During 2013, just under 20% of all breaches experienced by DBIR participants were detected internally, with the remainder identified by third-party notification. Likewise, our respondents are focused on improving detection first, decreasing the number of days an attacker spends in an environment undetected.

Improving response time is a goal for 42% of respondents over the next two years. Typically, as IR teams mature and detection improves, focus tends to shift to increasing the efficiency of the IR process, including data collection and correlation. Process refinement is likely a goal for more mature teams, though the integration that most respondents have planned with the SIEM will most likely have a positive effect on response time as well as detection.

[8] www.verizonenterprise.com/DBIR/2014

Recommendations

Armed with these survey results, it is clear that most organizations can achieve more efficient processes by implementing the following recommendations.

Better Define the Term *Incident*

Armed with an agreed-upon definition, it is much easier to add trackable metrics or key performance indicators (KPIs) for detection and remediation—something more likely to secure additional budget.

In the National Institute of Standards and Technology publication NIST SP 800-61,[9] the formal definition of an *incident* is "a violation or threat of violation of computer security policies, acceptable use policies, or standard security practices." Yet, in practice, organizations have different interpretations of what types of events this definition should include. With an overly broad definition of what falls into the category of *incident*, an IR team can quickly become overwhelmed with the triage, investigation and event handling that should not directly involve them. Moreover, armed with an agreed-upon definition, it is much easier to add trackable metrics or key performance indicators (KPIs) for detection and remediation—something more likely to secure additional budget.

A well-written IR policy, crafted in the preparation step of the six-step IR process, should include a formal definition of what incident types the IR team will be responsible for. Valuable resources can be tied up if the IR team is the victim of "scope creep" and tasked with investigating every employee acceptable use policy violation or tracking down lost or stolen equipment.

Prior to the charter of the IR team and development of its mission, all stakeholders must agree upon the definition of *incident*. Only with such agreement can staff accurately define the roles and responsibilities of the IR team. Those writing the policies and procedures should provide other details, such as conditions under which a member of the IR team can remove a system from the network or shut a system down. To be sure all parties are on the same page, be sure C-level executives sign off on the policy before it is implemented.

[9] "Computer Security Incident Handling Guide," http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

Build Security into Other Business Unit's Processes

Part of reducing an IR team's workload depends on other business units taking an active role in problem ownership. All data owners or people who manage/maintain an organization's information technology assets should receive training on implementing security best practices. Such training will ensure visibility of security efforts and buy-in from various units when a serious breach does occur.

By ensuring software developers include security considerations in their development cycle, the IR team will have fewer problems with vulnerable in-house applications and, subsequently, fewer incidents requiring response. Those desktop support technicians tasked with interfacing with an organization's user population must have a firm understanding of system triage and receive training so that they may properly differentiate between a user issue and a malware infection. Finally, data owners must understand the security gains associated with best practices such as least privilege required access and system and application event auditing. If security is "baked in" to daily business practices, the IR team will experience fewer critical incidents.

All data owners or people who manage/maintain an organization's information technology assets should receive training on implementing security best practices.

Track Incident Response Costs to Justify IR Tools and Larger Team

The survey asked participants whether they measure the costs associated with handling an incident, and only 14% affirmed that they do. Another 63% of respondents do not measure the cost, and 23% don't know (see Figure 17).

Do you measure the associated costs of handling incident response?

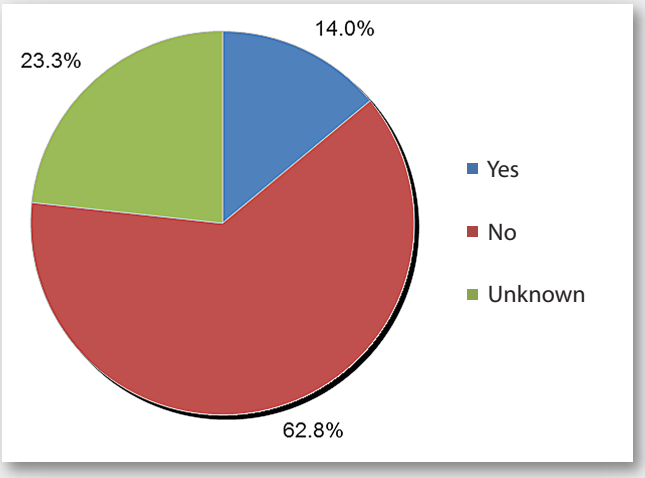


Figure 17. Measurement of IR Costs

Why is this a concern? Without accurate measurement of the costs involved in handling an incident, the budget for IR activities is almost certain to suffer. With a quarter of those who responded in managerial roles, the low visibility into cost information is indeed surprising.

One recommended technique for justifying additional resources such as staff, hardware and software is to track the costs of current inefficient processes and procedures. Generating metrics that support the need for additional budget allocation to fund staffing and enterprise IR tools will provide information to help upper management better understand future budgets requests. Putting a monetary value on the following metrics would be useful in justifying more resources: direct costs of engaging third-party forensic/IR services and travel costs for a responder to get to compromised systems when remote tools would have worked, indirect costs of decreased productivity of sourcing the department with surge staff during an incident, indirect costs of training surge staff and indirect costs of manually processing data/logs. By tracking the financial penalties to organizations that do not have adequate resources, security managers can make a persuasive argument to properly staff and equip their in-house IR capability.

Direct costs of engaging third-party forensics/IR services and travel for a remote responder, as well as indirect costs of decreased productivity of sourcing IR surge staff during an incident, training surge staff, and manually processing data and logs are metrics that are useful in justifying additional resources.

Enterprise IR tool rollout and maintenance fees can be a considerable line item in a security team's annual budget. Yet, if evaluated properly, these tools can simplify the tedious and time-consuming data acquisition process to enable smaller teams to respond more efficiently and thoroughly. The right IR tool can allow a team to do more with less and shave time off all stages of IR.

The survey also uncovered that 30% of respondents don't have any of their security budgets allocated for IR. Another 39% of respondents don't know whether they have any budget for IR (or how much it is). Figure 18 provides a look at the status of IR budgets.

What percentage of your security budget is assigned to incident response?

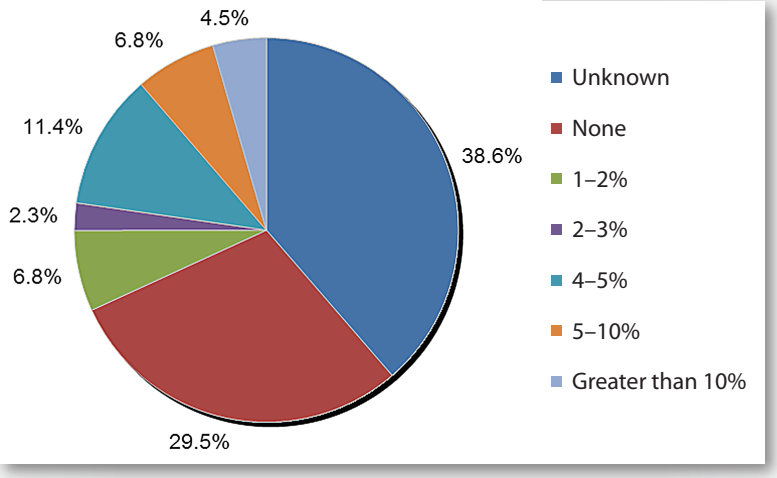


Figure 18. Percent of Security Budget Dedicated to IR

The demand for organizations to have a continuous monitoring and response capability makes dedicated IR teams imperative.

The consequences of not having a budget for IR or not having visibility into what that budget covers include the potential to lose current licenses or be unable to obtain licenses for essential software, including network- and host-based monitoring tools, forensics tool suites and data collection and parsing tools. Likewise, a lack of budget or an inability to secure appropriate funding for the constantly growing storage media needs of an IR team can result in a lack of historical data that may be needed to investigate a past vector of initial infection. Organizations must acknowledge the growing importance of this type of data as well as trained professionals who can interpret the data to retell the story of what happened.

Track Incident Response Metrics to Justify IR Tools and Increased Size

Most mature IR teams are achieving greater success in detection and containment by making use of proactive continuous monitoring and response rather than reactive intermittent response processes.

Despite the current security climate, 14% of respondents work in organizations with no dedicated IR teams. This lack of a formal team was cited as a key obstacle in efficient incident handling. Many security managers find it difficult to justify staffing full-time dedicated IR professionals, because the frequency or volume of an organization's incidents tend to be cyclical.

It is this intermittent nature of feast or famine that makes it hard for IR managers to justify permanent staff. Yet, most mature IR teams are achieving greater success in detection and containment by making use of proactive continuous monitoring and response rather than reactive intermittent response processes. The current recommendation is to view response as not occasional but continuous—with team members hunting for signs of intrusion or anomalies when they are not working on identified events. Performance metrics that may aid in the justification of additional team members or IR tools include tracking three time frames: the time from initial infection to detection, from detection to containment, and from detection to remediation.

About the Author

Alissa Torres is a certified SANS instructor specializing in advanced computer forensics and incident response. Her industry experience includes serving in the trenches as part of the Mandiant Computer Incident Response Team (MCIRT) as an incident handler and working on an internal security team as a digital forensic investigator. She has extensive experience in information security, spanning government, academic and corporate environments, and holds a bachelor's degree from University of Virginia and a master's from University of Maryland in information technology. Alissa has served as an instructor at the Defense Cyber Investigations Training Academy (DCITA), delivering incident response and network basics to security professionals entering the forensics community. In addition to being a GIAC Certified Forensic Analyst (GCFA), she holds the GCFE, GPEN, CISSP, EnCE, CFCE, MCT and CTT+ certifications.

Sponsor

SANS would like to thank this survey's sponsor:

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.