Research Insights Paper

Status Quo Creates Security Risk: The State of Incident Response

By Jon Oltsik, Senior Principal Analyst

February 2016

This ESG Research Insights Paper was commissioned by ServiceNow and is distributed under license from ESG.

Contents

Executive Summary

In late 2015 and early 2016, the Enterprise Strategy Group (ESG) conducted a research survey of 184 IT and cybersecurity professionals with knowledge of, responsibility for, or day-to-day operational oversight of incident response processes and technologies at their organizations. Survey respondents were also required to spend at least 25% of their time on incident response processes and technologies on a daily basis.

Survey respondents were located in North America and came from organizations ranging in size: 19% of survey respondents worked at organizations with 1,000 to 4,999 employees, 36% worked at organizations with 5,000 to 9,999 employees, 21% worked at organizations with 10,000 to 19,999 employees, and 24% worked at organizations with 20,000 or more employees. Respondents represented numerous industry and government segments with the largest participation coming from the manufacturing industry (18%), business services (16%), financial services (15%), information technology (11%), and retail/wholesale (11%).

This research project was undertaken in order to evaluate the current practices and challenges associated with incident response processes and technologies. Respondents were also asked to provide details on their organizations' future strategic plans intended for improving the efficacy and efficiency of IR activities. Based upon the data collected as part of this project, this paper concludes:

- **Incident response depends upon strong collaboration between cybersecurity and IT operations teams.** When asked to identify the most important factors for incident response excellence, 31% of survey respondents pointed to security and IT tools integration while 24% said strong collaboration between cybersecurity and IT operations teams. Furthermore, 70% of organizations say the incident response processes are tightly aligned with IT operations frameworks and guidelines like COBIT, ITIL, and NIST. When it comes to incident response quality, cybersecurity professionals believe there must be a clear symbiotic relationship between cybersecurity and IT teams.
- **Many organizations identify organizational challenges.** While survey respondents were quick to point to the need for cybersecurity and IT collaboration, many say that their organizations have challenges in these areas. One-third (33%) of organizations say they are challenged in coordinating IR activities between cybersecurity and IT operations teams, while 30% claim that they find monitoring incident response processes from end-to-end (i.e., through detection, investigations, ticketing, and response) especially challenging.
- **IR is fraught with manual processes**. When asked if their organization's incident response efficiency and effectiveness is limited by the time and effort required for manual processes, 93% of the cybersecurity professionals surveyed responded, "yes." This is a real problem since 22% of organizations find it challenging to keep up with the volume of security alerts. As security alert volume inevitably increases over time, manual process bottlenecks will greatly impact large organizations' abilities to scale IR processes.
- **CISOs are adopting IR automation and orchestration to address current problems.** Over 90% of organizations are doing technical integration or deploying new technologies intended to help them automate and orchestrate IR processes. Survey respondents say that their organizations are embracing IR automation and orchestration to improve detection/response times, improve collaboration between cybersecurity and IT teams, and allow them to automate simple remediation tasks.
- **Enterprises have aggressive IR plans.** A vast majority (88%) of organizations plan to increase spending on incident response over the next two years. In addition to budget growth, 47% of organizations plan to improve the alignment of incident response and IT governance processes, 42% want to consolidate incident response personnel and tools into a common location, 39% plan to create a formal CERT, and 34% intend to provide more IR training to cybersecurity and IT operations teams.

Situational Analysis of Incident Response

For the purposes of this research project, incident response was defined as follows:

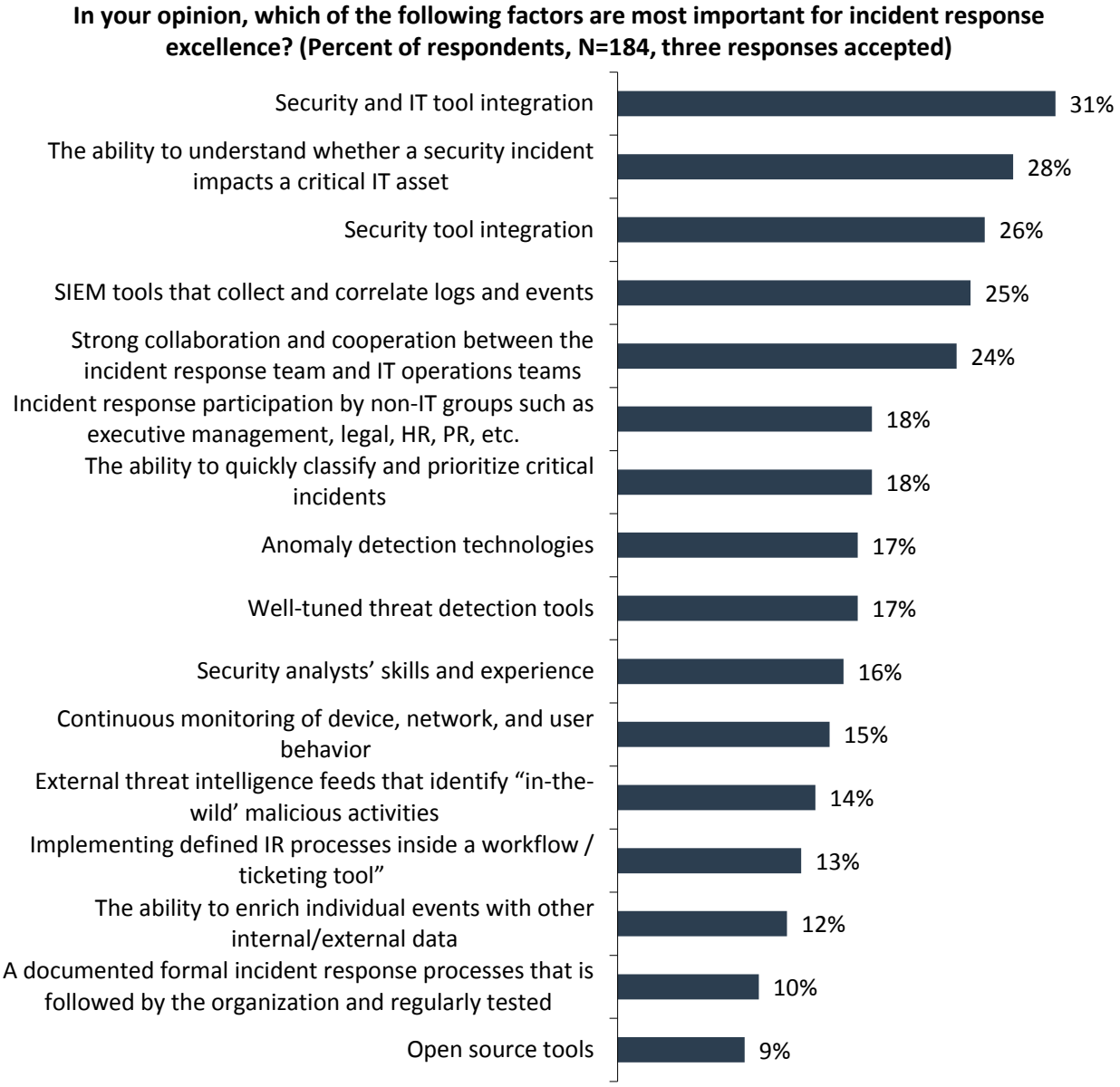
> *An organized approach to addressing and managing the reaction to a discovered risk (i.e., threat or vulnerability), security breach or cyber-attack. The goal of incident response is to quickly detect and remediate all aspects of any type of security incident in a way that limits damage, reduces recovery time, and minimizes costs.*

Based upon this definition, survey respondents were asked to identify the most important factors that lead to incident response excellence (see Figure 1). Cybersecurity professionals point to many things including:

- **Security and IT tool integration.** Nearly one-third (31%) of cybersecurity professionals recognize the holistic nature of incident response that spans across infosec and IT operations teams. Therefore, survey respondents believe that IR excellence must be anchored by strong interoperability and a common view across all cybersecurity and ITSM technology components. Security and IT tool integration can allow cybersecurity and IT operations to work together seamlessly to detect and respond to security events in an efficient manner.
- **The ability to know whether a security incident impacts a critical system.** All security incidents are not created equally. Some can impact a low-priority user PC while others take aim at business-critical applications and databases. More than one-fourth (28%) of cybersecurity professionals believe that true IR excellence must be based upon the ability to distinguish between pedestrian events and those that could disrupt business operations or seek to steal sensitive intellectual property (IP), leading to a devastating data breach.
- **Strong collaboration between the incident response and IT operations teams.** Aside from technology integration alone, 24% of survey respondents claim that IR excellence depends upon strong collaboration between incident response and IT operations teams. When security analysts identify an issue on IT ticketing systems, they need the IT operations team to work in concert with them to prioritize the event, quarantine systems, and take immediate remediation actions.

On a similar train of thought, 18% of cybersecurity professionals believe that IR excellence includes the ability to quickly classify and prioritize security incidents. This is certainly associated with technology integration and cooperative processes.

Figure 1. Important Factors for Incident Response Excellence



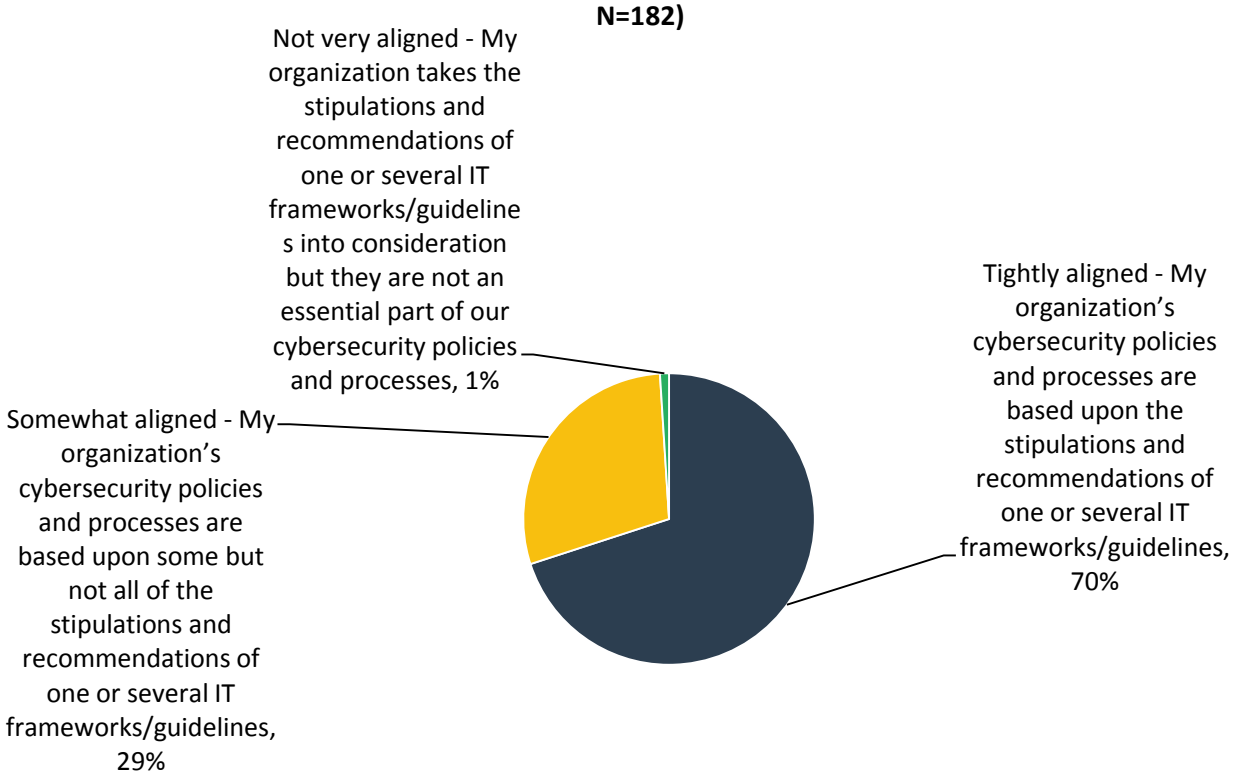
Source: Enterprise Strategy Group, 2016.

Since IR excellence depends upon a foundation of close collaboration between cybersecurity and IT operations, it is no surprise that 70% of organizations say that incident response is tightly aligned with IT governance frameworks and guidelines (see Figure 2).

This may be a positive sign for incident response. Many enterprise organizations have years of experience and millions of dollars invested in IT operations frameworks like COBIT, ISO 20000, ITIL, and the Microsoft Operations Framework (MOF) in order to systematize IT processes like configuration management, change management, and service management. Alternatively, incident response is often managed more informally by key individuals using their own methodologies. ESG believes that tight integration could force IR processes to adhere to the discipline and rigor applied to IT service management. This could then lead to improvements in IR productivity, efficacy, and efficiency.

Figure 2. Alignment Between Cybersecurity and IT Frameworks and Guidelines

You indicated that your organization uses one or several IT governance frameworks/guidelines. In your opinion, how closely aligned are your organization's cybersecurity policies and processes with policies and processes stipulated in these IT frameworks/guidelines? (Percent of respondents, N=182)



Source: Enterprise Strategy Group, 2016.

IR Issues and Challenges

Cybersecurity professionals believe that technology integration, collaboration between cybersecurity and IT operations, and tight alignment between cybersecurity and IT operations frameworks are important components for their incident response performance. Unfortunately, security professionals admit to one or several problems in these and other IR areas. For example (see Figure 3):

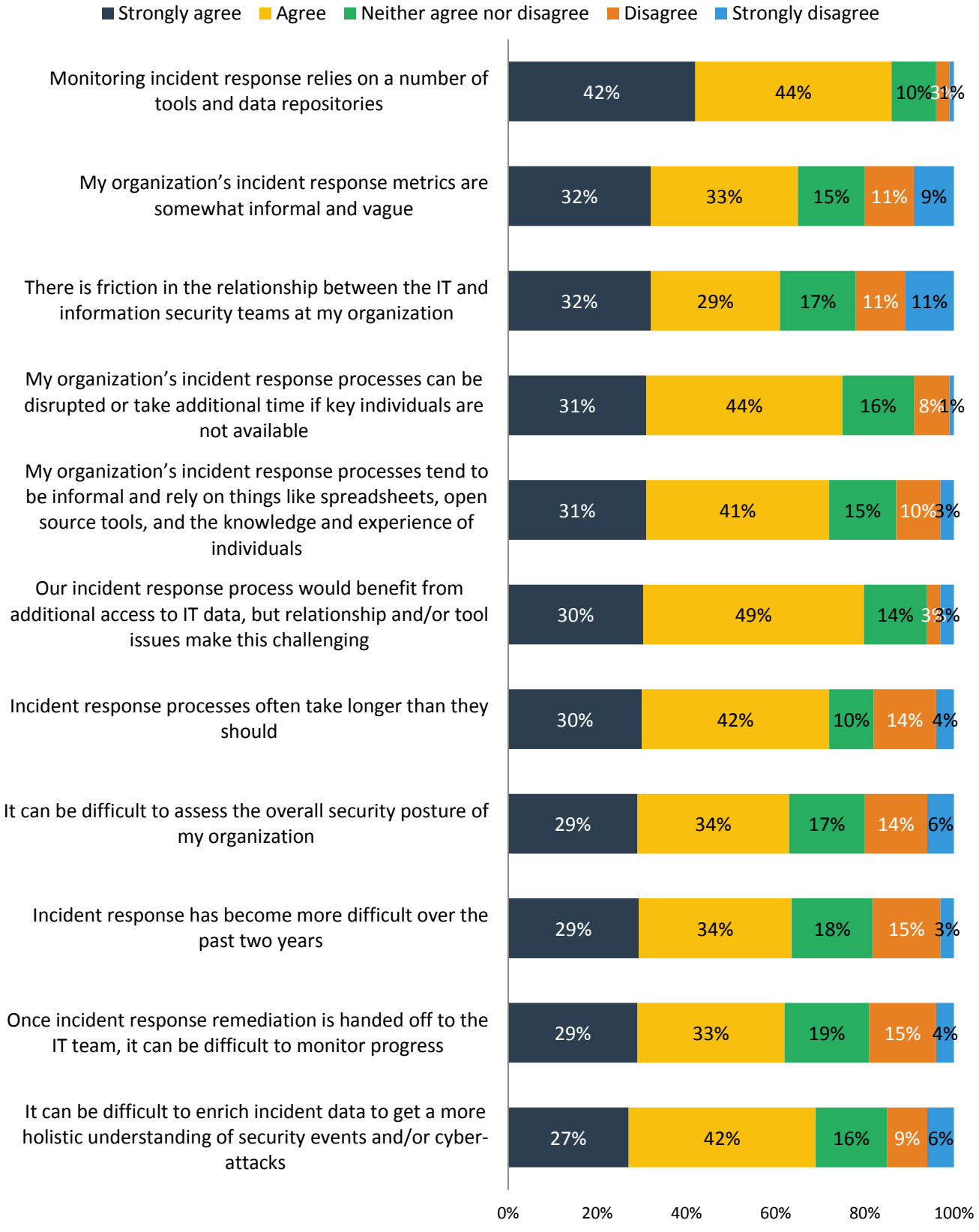
- Seventy-two percent of survey respondents "strongly agree" or "agree" that IR processes tend to be informal and reliant on things like spreadsheets, open source tools, and the knowledge and experience of individuals. Additionally, 75% believe that IR processes can be disrupted if key individuals are unavailable. So in spite of the fact that organizations tightly integrate cybersecurity processes with IT operations frameworks and guidelines, IR remains somewhat undisciplined and haphazard. The impact of these issues tends to increase as the volume of systems on the network, network traffic, and security alerts escalate.
- Sixty-nine percent of survey respondents "strongly agree" or "agree" that it can be difficult to enrich data to get a more holistic understanding of security alerts and/or cyber-attacks. In incident response, data enrichment means combining data sources for a more complete picture. For example, a security analyst might want to enrich data from a network anti-malware sandbox with data from endpoint forensics tools, threat intelligence feeds, and IT asset data from a CMDB. This can be difficult as it is often based on a series of manual and time-consuming processes. This is not only inefficient but also adds to the dwell time for cyber-attacks.
- Sixty-one percent of survey respondents "strongly agree" or "agree" that there is some friction between the information security and IT operations teams at their organizations. Based upon the data presented previously in this paper, cybersecurity professionals clearly believe that IR process quality depends upon

sound communications and collaboration between cybersecurity and IT operations teams. Unfortunately, these relationships can be strained—61% agree that friction exists between these groups. This friction is often experienced during the handoff for system remediation from SOC teams to IT operations, elongating timeframes, increasing dwell time for malware, and increasing IT risk. This may be why 62% of survey respondents agree that incident response processes often take longer than they should.

It is also worth noting that 63% of survey respondents agree with the statement, "Incident response has become more difficult over the past two years." Rather than improving, it is safe to assume then that many of these issues continue to get worse over time.

Figure 3. Cybersecurity Professionals' Opinions on Incident Response at Their Organizations

Please indicate whether you agree or disagree with each of the following statements. (Percent of respondents, N=184)



Source: Enterprise Strategy Group, 2016.

ESG also asked cybersecurity professionals to identify specific incident response challenges at their organizations. Survey respondents pointed to numerous problems such as (see Figure 4):

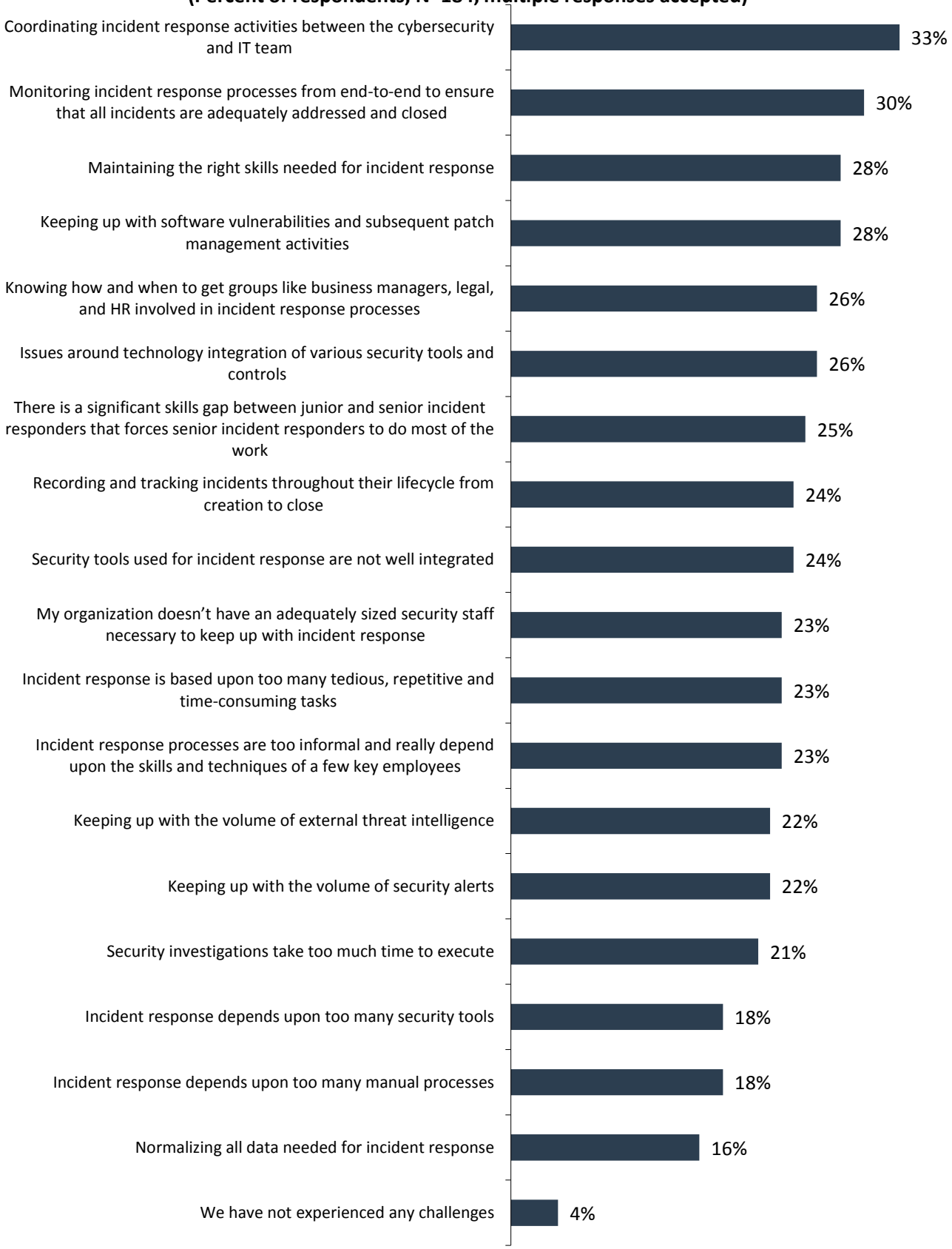
- **Coordinating IR activities between cybersecurity and IT teams.** This topped the list once again as one-third of survey respondents' view this as a challenge.
- **Monitoring IR processes from end-to-end.** Thirty percent of survey respondents find it challenging to monitor end-to-end IR processes—from detection, through security investigations, to remediation and problem closure. This is likely due to the lack of cybersecurity and IT operations tools integration as well as friction between these two groups.
- **Maintaining the right IR skills.** Many aspects of IR require experienced security analysts who can conduct forensic investigations, dissect malware, or fine-tune security controls to prevent sophisticated attacks, which is why 28% of organizations are challenged with maintaining the right IR skills. Unfortunately these skills are in short supply. According to other ESG research, 46% of organizations claim to have a "problematic shortage" of cybersecurity skills and 87% believe it is difficult to recruit and hire cybersecurity talent.[1] To maintain the right incident response skills, CISOs must hire and train junior security analysts and invest in advanced training to keep senior SOC staff up to speed. This process requires time, money, and constant diligence.
- **Knowing when to get other groups involved.** The ESG data indicates that 26% or respondents have trouble knowing how and when to get groups like business managers, legal, and HR involved with IR processes. This should be expected given that IR processes are often informal in nature but this issue can lead to real problems. When the CERT discovers a data breach that resulted in the exfiltration of medical records and customer data, organizational reputation, share price, and legal protection can depend upon the execution of a well-tested plan that includes actions like alerting customers, working with law enforcement, and communicating with the press. Clearly, these are NOT cybersecurity or IT operations tasks but they are indeed essential to incident response.
- **Keeping up with security alerts.** Twenty-two percent of enterprises find it challenging to keep up with the volume of security alerts they receive on a daily basis. Since this volume is only increasing, this should be especially concerning to CISOs.

Finally, recall that 31% of cybersecurity professionals indicated that cybersecurity and IT operations tool integration is a key factor for incident response excellence. Sadly, more than one-fourth (26%) report issues around technology integration of various security technologies and controls.

[1] Source: ESG Brief: *Cybersecurity Skills Shortage: A State of Emergency*, February 2016.

Figure 4. Incident Response Challenges

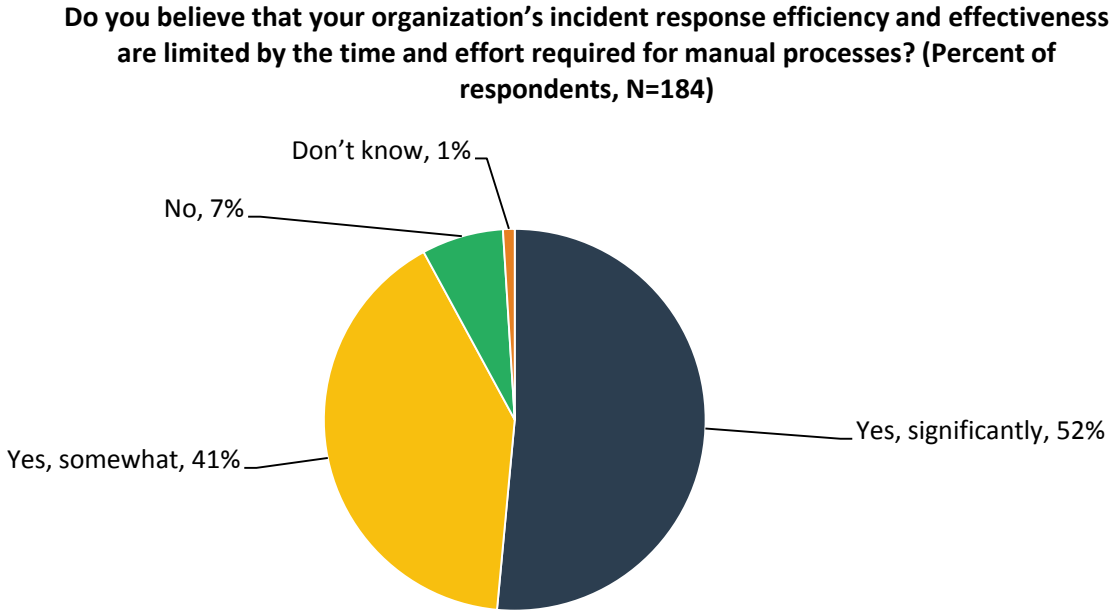
In your opinion, what are the biggest incident response challenges at your organization? (Percent of respondents, N=184, multiple responses accepted)



Source: Enterprise Strategy Group, 2016.

Aside from the challenges described above, cybersecurity professionals also admit that manual processes get in the way of IR efficiency and effectiveness (see Figure 5). This alone creates an alarming scenario for the future as manual processes can't possibly keep up with the growing volume of security alerts or help CISOs improve collaboration between cybersecurity and IT operations teams.

Figure 5. Manual Incident Response Processes Hinder Efficiency and Effectiveness

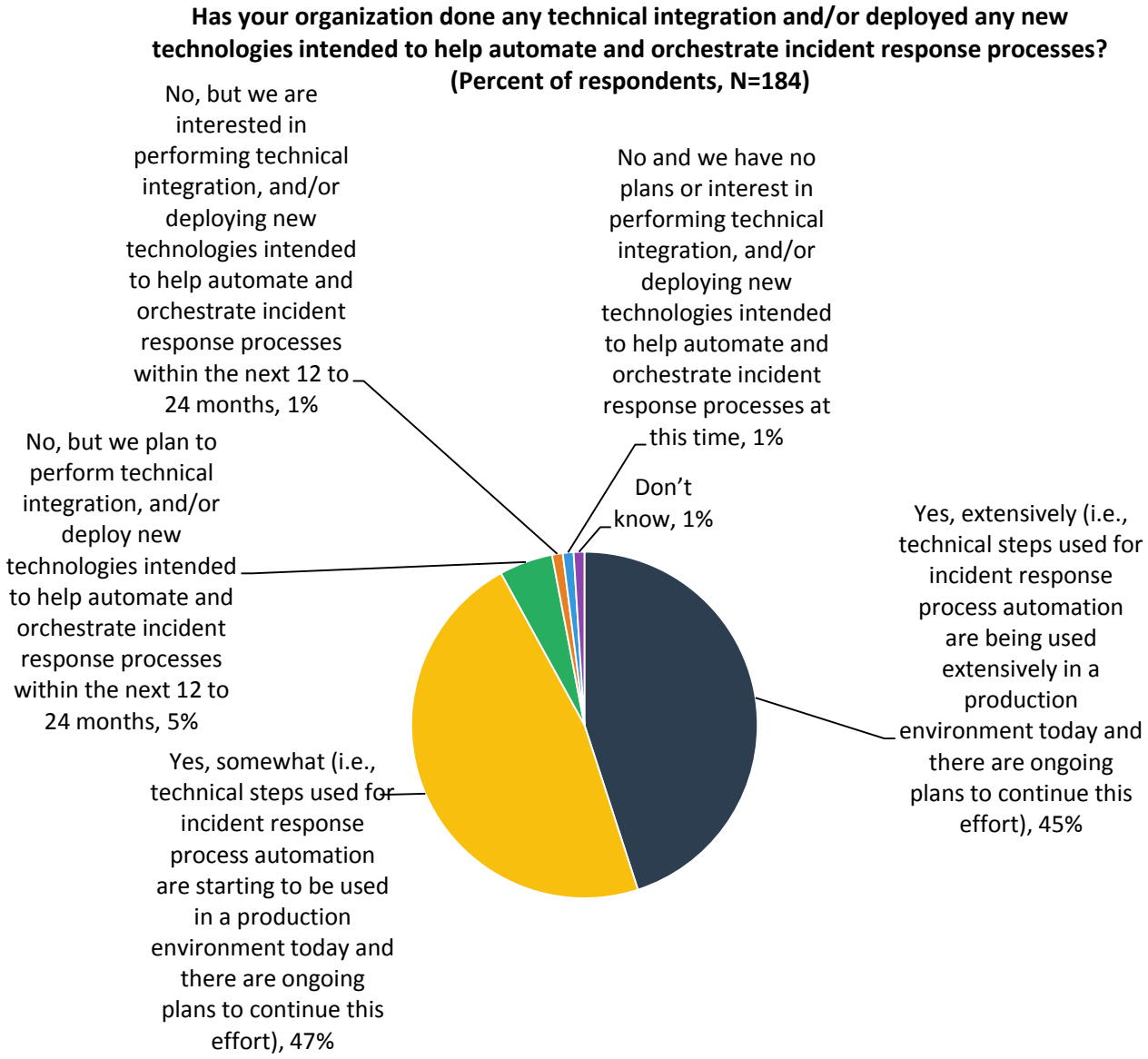


Source: Enterprise Strategy Group, 2016.

IR Efficiency Needs Improvement

The ESG data reveals that incident response processes are frequently characterized by manual processes, a lack of technology integration, and friction between SOC and IT operations teams. Concerned CISOs realize that they need to address these issues as soon as possible in order to accelerate and improve IR efficiency while optimizing the productivity of their personnel. Given the global cybersecurity skills shortage, many security executives have come to understand that the best way forward is to formalize, automate, and orchestrate IR processes. Many organizations are doing exactly this—45% of organizations are automating and orchestrating IR processes extensively while another 47% are doing so somewhat (see Figure 6).

Figure 6. Enterprise Organizations Are Moving Toward IR Automation and Orchestration



Source: Enterprise Strategy Group, 2016.

Why do so many organizations want to automate and orchestrate their IR processes? Cybersecurity professionals cite several reasons including the following (see Figure 7):

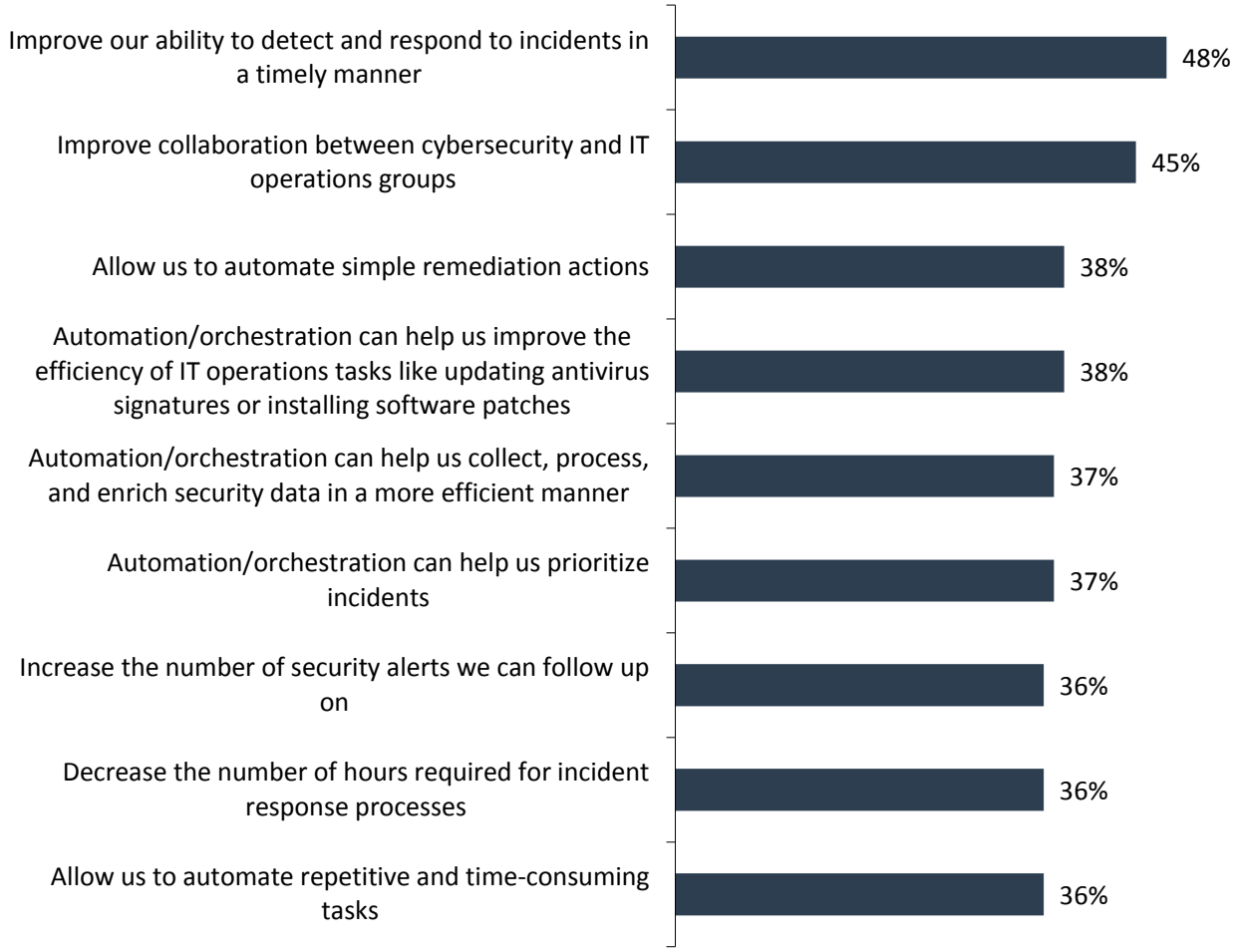
- Forty-five percent want to use IR automation and orchestration to improve collaboration between cybersecurity and IT operations groups. In this case, automation/orchestration can add structure to cross-group communications and help alleviate process bottlenecks when remediation tasks are handed off from security analysts to IT operations teams.
- Thirty-eight percent believe that IR automation/orchestration can help them improve efficiency of IT operations tasks like updating antivirus signatures or installing software patches. Enterprises have no shortage of these types of day-to-day tasks with countless manual steps involved. Automation/orchestration can help them save time, improve the time it takes for end-to-end workflows, and bolster productivity.
- Thirty-seven percent want to use IR automation/orchestration to help them prioritize incidents. In other words, IR automation and orchestration can help them deal with security alert volume, enrich data

elements, and make decisions on which security incidents need immediate attention and which get a lower ranking.

- Thirty-six percent want to use IR automation and orchestration to help them decrease the number of hours needed for incident response processes. CISOs clearly realize that the combination of increasing security alerts and a global cybersecurity skills shortage puts them in a difficult position. They see IR automation/ orchestration as their best hope for increasing productivity in order to keep up.

Figure 7. Why Organizations Are Automating and Orchestrating Incident Response Processes

You indicated that your organization has taken actions to automate and/or orchestrate incident response processes or is planning to do so or interested in doing so in the future. Why has or will your organization do this? (Percent of respondents, N=182, multiple responses accepted)

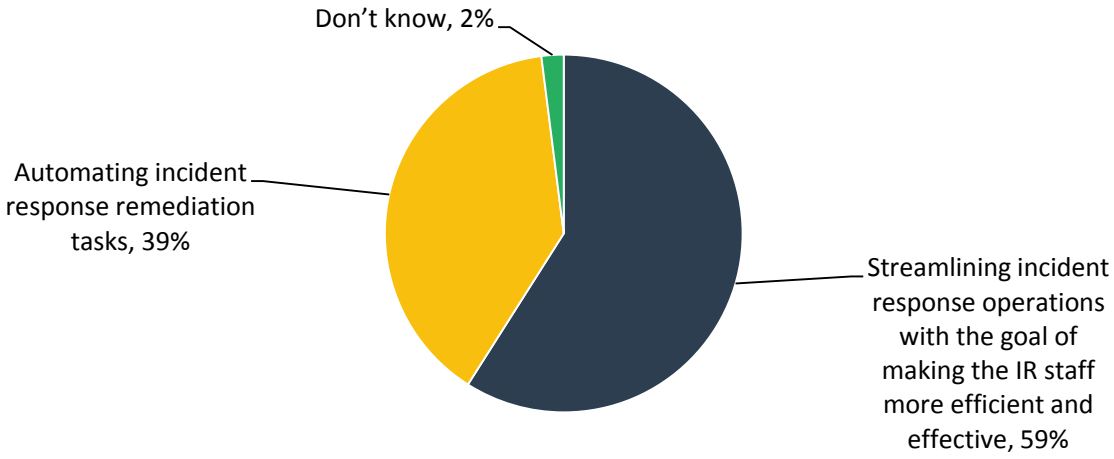


Source: Enterprise Strategy Group, 2016.

As far as automation and orchestration priorities, 59% want to start by streamlining incident response operations with the goal of making the IR staff more effective and efficient (see Figure 8). In other words, CISOs believe they need to start by improving collaboration between CERTs and IT operations and making IR processes more like the formal methodologies they employ using IT operations frameworks like COBIT, ISO, ITIL, and NIST.

Figure 8. Incident Response Automation and Orchestration Priorities

In your opinion, which is the higher priority for incident response automation/orchestration at your organization? (Percent of respondents, N=184)



Source: Enterprise Strategy Group, 2016.

Next Steps

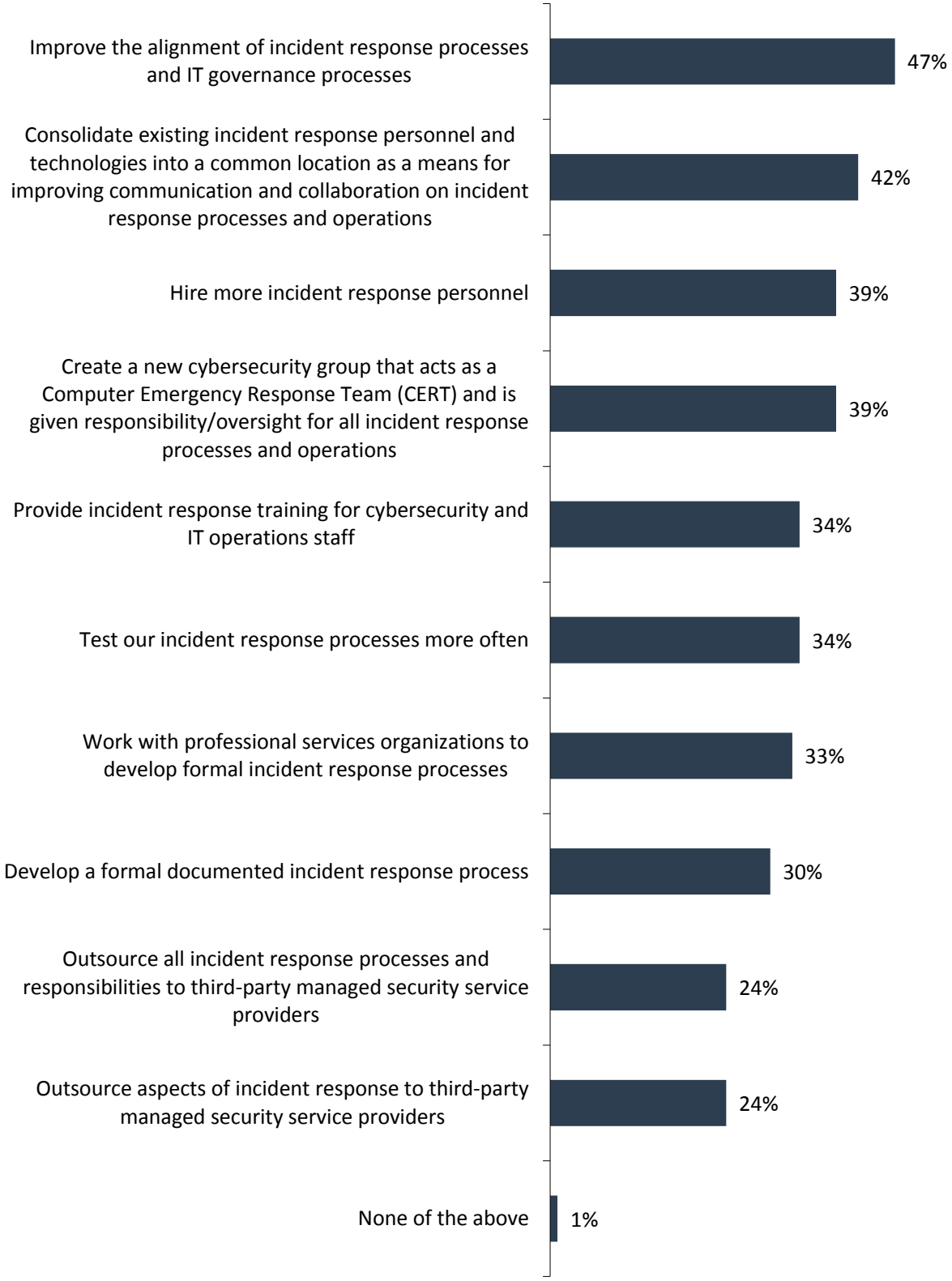
Over the next two years, 46% of organizations say that incident response spending will increase significantly while 42% claim that IR spending will increase somewhat during this timeframe. This indicates that most enterprise CISOs believe they need to invest in people, processes, and technologies to improve IR efficacy, efficiency, and productivity.

In addition to budget increases, cybersecurity professionals described a number of actions their organizations will take as part of their incident response strategy in the future, including (see Figure 9):

- Forty-seven percent plan to improve the alignment of incident response and IT governance processes. Recall that 70% of organizations say that their cybersecurity processes are tightly aligned with IT operations frameworks and guidelines. While this represents a majority, it appears that CISOs and CIOs want to make these relationships even tighter with a likely goal of improving cross-organizational collaboration, formalizing IR processes, and defining the right metrics to track for continuous improvement. This objective is further evidenced by the fact that 42% of organizations want to develop formal and documented IR processes.
- Forty-two percent plan to consolidate existing IR personnel and technologies into a common location as a means for improving communication and collaboration related to incident response processes and operations. Note that 39% want to create a CERT as well. In both cases, organizations want to build more structured incident response teams to address many of their current organizational challenges.
- Thirty-four percent plan to provide IR training to cybersecurity and IT operations staff. This effort is meant to keep up to date with IR skills and get the IT operations staff more involved with end-to-end IR processes. ESG sees this as complementary to improving the alignment of IR processes with IT governance.

Figure 9. Strategic Cybersecurity Plans for Incident Response

As part of its cybersecurity strategy, will your organization take any of the following actions with regards to incident response over the next two years? (Percent of respondents, N=184, multiple responses accepted)



Source: Enterprise Strategy Group, 2016.

The Bigger Truth

The ESG data presented in this research report is something of a paradox. Cybersecurity professionals understand that incident response depends upon technology integration, cross-organization collaboration, and the ability to detect and prioritize security incidents, yet these are the very areas where they struggle today. This means that as security alert volume increases, enterprises will find themselves falling further behind, increasing cyber-attack dwell time and IT risk.

Enterprises seem to comprehend the seriousness of this situation as many organizations are increasing IR budgets, training personnel, and collocating IR tools and personnel to create a dedicated CERT. In addition, the vast majority of organizations are also automating and orchestrating incident response processes today or are planning to do so in the near future.

As organizations proceed with IR automation and orchestration, CISOs should study the progress made in IT service management over the last decade as there are many best practices and lessons learned that can be applied to cybersecurity as well. For example, CISOs should:

- **Focus efforts around high-value IT assets.** IR process improvement should ultimately culminate on better visibility and accelerated response time toward high-value IT assets like critical servers, applications, and sensitive data. CISOs should enlist the help of CIOs and IT operations to find and specify these resources, identify all data sources used for monitoring and threat detection, establish hardened configuration, and create formal escalation processes across cybersecurity, IT, and the business at large. Everyone should know how to identify problems, roles and responsibilities, and next steps with centralized communication and workflows with all other constituencies as IR tasks proceed.
- **Map out IR processes from end-to-end.** This involves assessing and documenting every IR task and step regardless of how miniscule each one seems. Once these processes are documented, it's important for CISOs to pass these runbooks by several senior members of the cybersecurity team to see if anything has been missed. Additionally, CISOs should review documented IR processes with IT operations to identify where ITSM tools and methodologies can be added to help with incident detection or response. Armed with comprehensive and documented IR process maps, CISOs can then categorize where automation and orchestration can be applied to eliminate manual steps and deliver immediate value. These process maps can also be used to free up time for the security staff to work on high-priority needs.
- **Provide a common dashboard for cybersecurity and IT operations teams.** One of the big issues identified in this research project was the lack of integration between cybersecurity and IT operations tools, so addressing this issue should be a high priority. In the short term, CISOs will want to align workflows to data sources and use product APIs for data access and exportation. This will give the SOC team the ability to pivot from one data point to another without the need to go through individual tools management systems. CISOs may opt to centralize IR process monitoring in the future by creating common reports and dashboards for viewing by CERT and IT operations teams as well. A common view can certainly help ameliorate today's cross-organizational friction.
- **Define and track IR metrics.** In the struggle to keep up with the volume of security alerts, many organizations aren't doing enough to actually define and track IR metrics. Automation and orchestration can certainly help here. Since IR relies on a foundation of people and process, CISOs should start with key performance indicators focused on boosting productivity of the IR and IT operations staff, such as the number of incidents investigated by junior analysts, the number of investigators per analyst, response time for emergency actions, and response time for lower priority events. The goal should be overall effectiveness balanced against productivity. It is also important to establish internal service level metrics to set and track IR goals and objectives.
- **Make sure IR automation and orchestration support regulatory compliance and IT audits.** Aside from IR alone, automation and orchestration should also be used for overall risk management—especially as it

relates to regulatory compliance. This can be as simple as automating data collection for day-to-day reporting and should also support automating post-incident response reporting.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0218 | www.esg-global.com