AT&T Cybersecurity

A thought leadership report from AT&T Cybersecurity

Published 5 May 2020

The Relationship Between Security Maturity and Business Enablement

A Benchmark Report Exploring the Impact of Cybersecurity Maturity on Business Outcomes

AT&T Business

Contents

Executive Summary

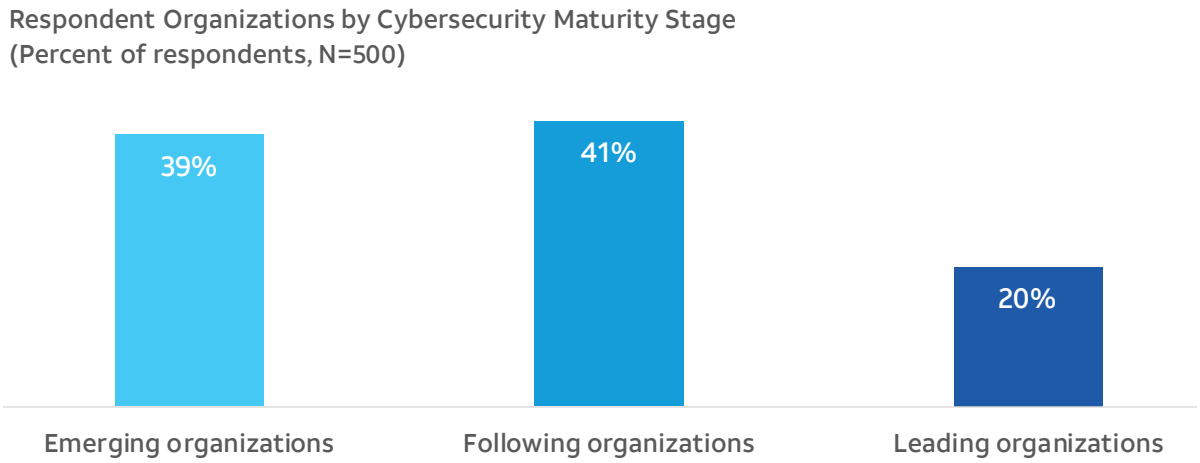
In March 2020, AT&T Cybersecurity, in partnership with industry analyst firm, the Enterprise Security Group (ESG), completed a research survey of 500 cybersecurity and IT professionals who are directly involved with their organization's cybersecurity strategies, controls, and operations. Further description of the research methodology and survey demographics are presented in the appendix of this report. This research project was intended to parallel the National Institute of Standards and Technology (NIST) cybersecurity framework (CSF) by assessing organizations' postures across the five foundational cybersecurity functions of the CSF: Identify, Protect, Detect, Respond, and Recover.

The goal of the research was to validate if, and to what degree, organizations more in alignment with best practices prescribed by the NIST CSF can help to operate more secure environments and better enable their businesses. This was accomplished through the creation of a data-driven model that segments respondents into three levels of cybersecurity maturity: "emerging" organizations, "following" organizations, and "leading" organizations. By comparing survey results across these levels, the model allows us to use data to quantify the differences in security and business outcomes that exist as maturity level improves.

AT&T Cybersecurity's maturity model used 16 questions from the survey as inputs in the model which determined an organization's maturity score. These 16 questions measured a broad set of cybersecurity processes, policies, and controls in use by the organization. How formalized is the organization's cybersecurity program? How frequently does it provide cybersecurity training to users? How diligently does it identify and prioritize threats? How is threat intelligence brought to bear? How extensively are data and assets segmented and encrypted? What technologies are used in event identification and resolution? How often is the organization's security posture evaluated and revised over time? Based on the answers to these and other questions, respondents' organizations could earn between 0 and 100 maturity points.

The organizations represented by the lowest scoring 39% of respondents were placed in the least mature "emerging" category, organizations in the middle of the pack were placed in the "following" category, and those that comprised the top 20% of scores were placed in the "leading" category. See Figure 1 and Appendix II: Established levels of cybersecurity maturity used in this report for more details.

Figure 1: The Current State of Cybersecurity Maturity



Based upon the research, ESG believes that "leading" organizations can weave strong cybersecurity into the business, IT, and organizational culture.

Based upon the research collected for this project, AT&T Cybersecurity and ESG reached the following conclusions:

The data suggests a relationship between business success and a commitment to strong security. Based upon the research, ESG believes that "leading" organizations can weave strong cybersecurity into the business, IT, and organizational culture. This helps them be more aggressive with IT-driven business initiatives, knowing they can count on a strong security foundation.

"Leading" organizations tend to be further along in the five functions of the NIST CSF. This is particularly true in areas such as threat detection and incident response, where many "emerging" and "following" organizations struggle. Furthermore, "leading" organizations know their limitations and actively seek help from service providers to supplement internal staff and skills.

Despite their successes, "leading" organizations understand that security is a journey and not a destination. Therefore, they constantly assess progress, pinpoint areas of need, and strive for continuous improvement. So, while "leading" organizations spend more on security, they report stronger return on investment (ROI) on security investments. "Following" and "emerging" organizations can use the data presented in this report to better understand lessons learned and best practices of "leading" organizations. This can then serve as a roadmap for security improvement and business affinity.

Maturity is not directly dependent on company size. One might assume only the largest organizations, with the most resources, would be able to implement a cybersecurity program sophisticated enough to achieve "leading" status. However, the research shows that the median company size is identical across all three maturity levels – "leading", "following", and "emerging" organizations. The fact that there is no correlation between company size and maturity level indicates to us that doing cybersecurity well is less a function of resources and more a function of thoughtful consideration, planning, and organizational culture. While technology and staff investments matter, the research indicates that organizations of any size can achieve a highly mature cybersecurity program.

Research points to a correlation between strong security and business success

The research points to a relationship between business success and cybersecurity acumen. This connection is likely anchored by trust, communication, and collaboration between people—managers and staff from lines of business (LOB) and cybersecurity teams. Just over one-quarter (26%) of respondents say that security is viewed as an enabler by line-of-business stakeholders. When this data is viewed through the maturity model, however, security teams are seen as "enablers" by LOBs at 55% of "leading" organizations. Alternatively, 28% of LOBs view security as "a necessary inconvenience/roadblock" at "emerging" organizations (see Figure 2). Clearly, "leading" organizations are doing something right.

It is also noteworthy that 73% of "leading" organizations strongly agree with the notion that their organization's security posture makes their overall business success much more likely (see Figure 3). Of course, this is a subjective assessment, but this opinion seems to be supported by other data gathered for this research project. Security professionals at "leading" organizations tend to think of themselves as business enablers with a productive working relationship between the business and security teams. In this scenario, security teams focus their attention on understanding business processes and then identifying, mitigating, and monitoring related cyber-risks.

Figure 2: The Business's Perception of the Security Team, by Cybersecurity Maturity

In general, how would you characterize the way your organization's line-of-business stakeholders currently view the cybersecurity team? (Percent of respondents)

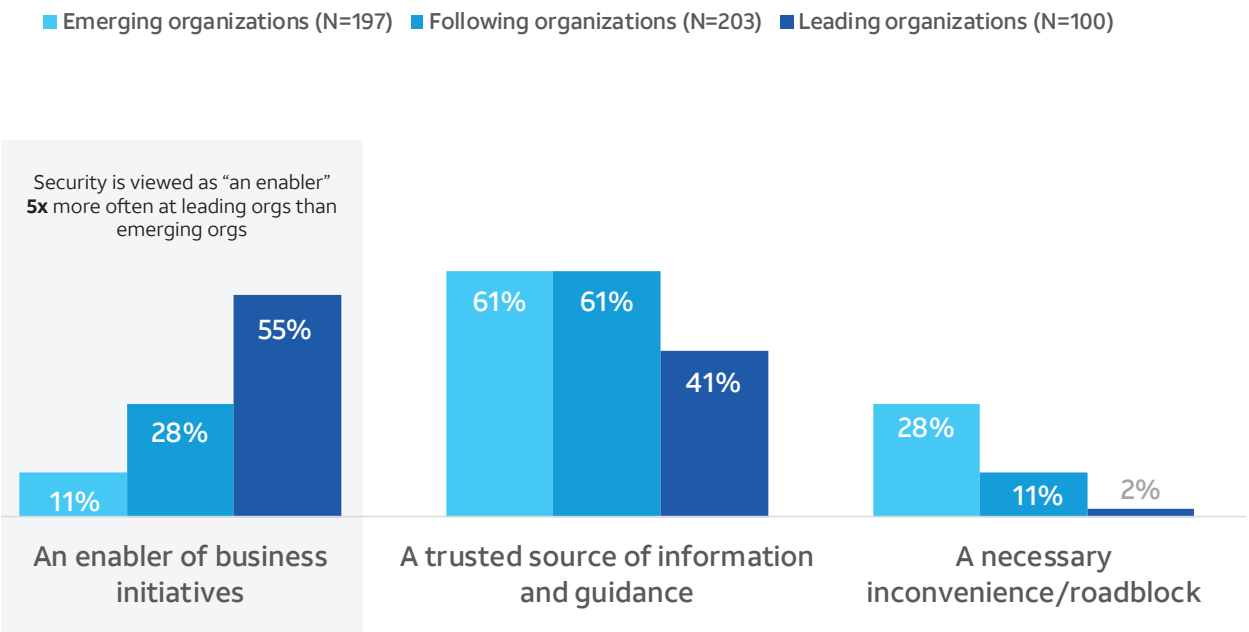
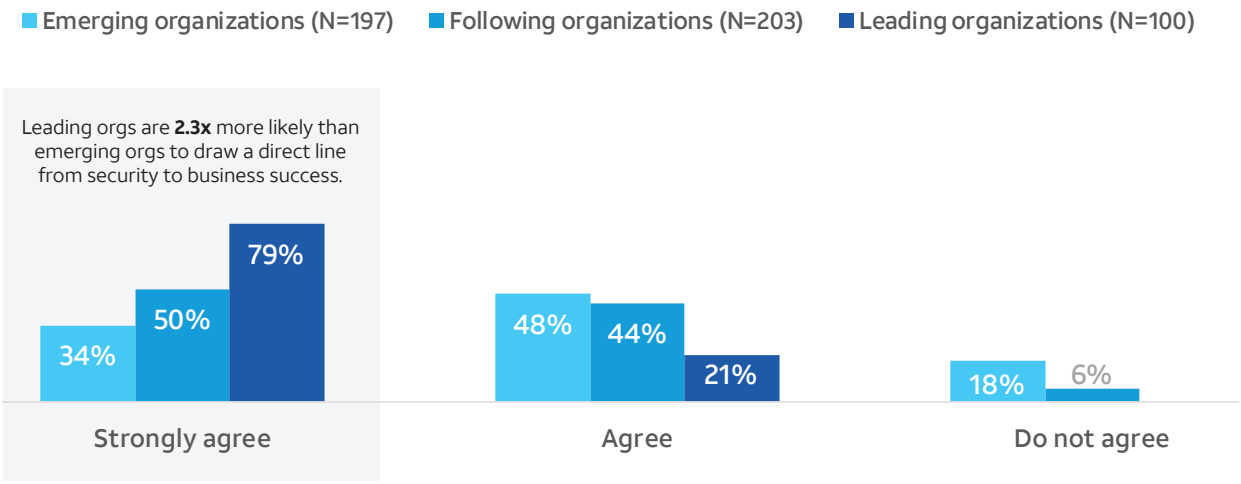


Figure 3: Perception that Security Drives Business Success, by Cybersecurity Maturity

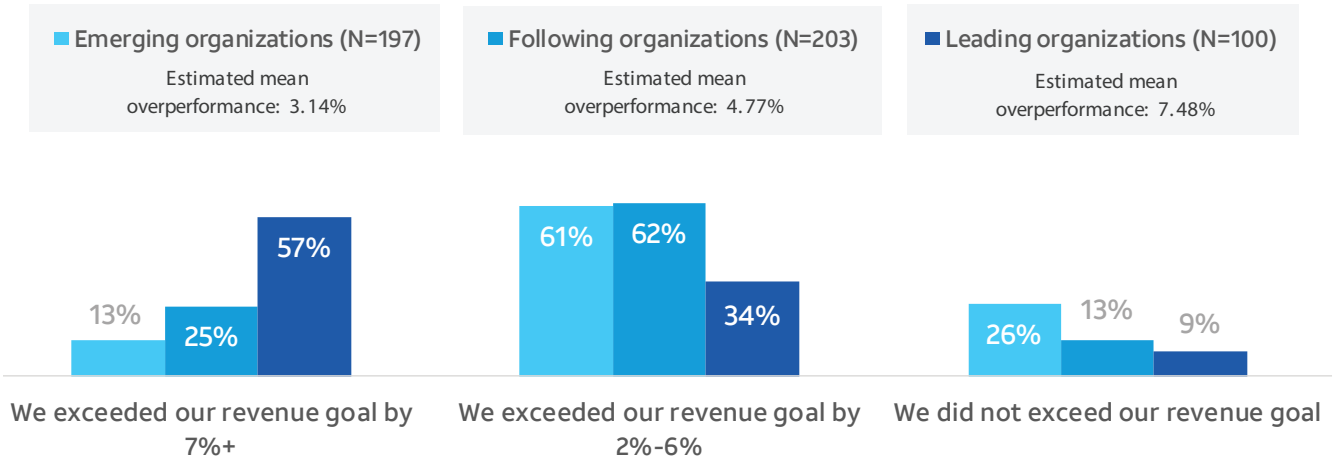
Please rate your level of agreement with the following statement:
My organization's security posture makes our overall business success much more likely
(Percent of respondents)



The research also indicates that organizations that commit to security tend to achieve greater success. This is not to suggest a causal relationship but rather that strong security can provide a foundation for organizations to be more aggressive with IT-driven business initiatives like digital transformation. For example, 57% of "leading" organizations claim to have exceeded revenue goals by 7%+ (see Figure 4). Beyond security, ESG postulates that these organizations have aggressive but well managed business plans supported by formal defined processes.

Figure 4: Organizations' Revenue Performance, by Cybersecurity Maturity

Thinking about your company's latest fiscal year (FY), which of the following represents its performance relative to its revenue goal? (Percent of respondents)



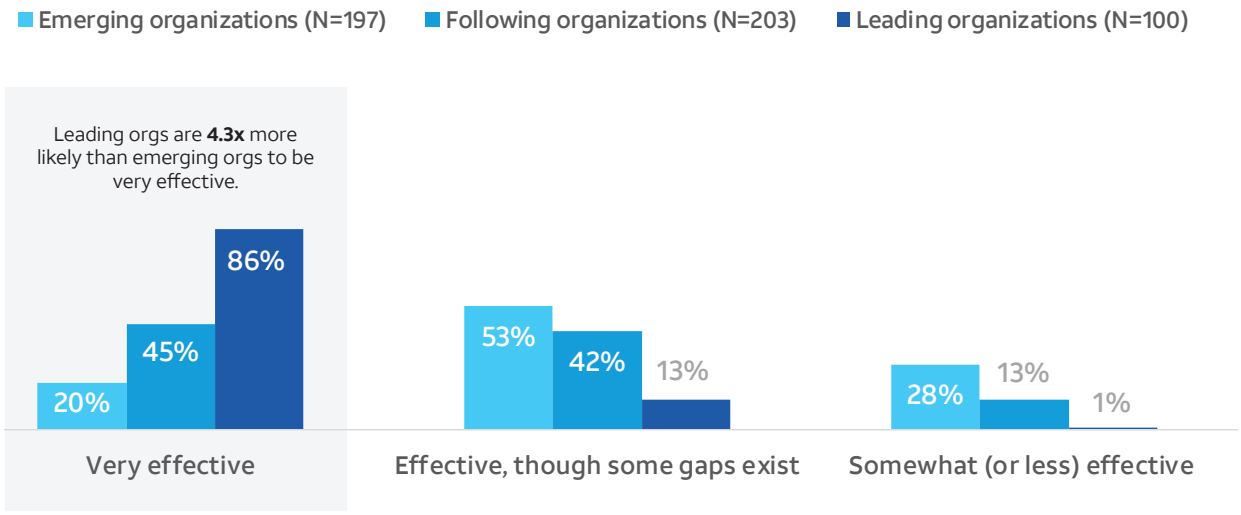
What makes a leader?

The research demonstrates a relationship between strong security and business success. This raises the question: What are the characteristics of a security "leader"? In other words, what actions do "leading" organizations take that make them stand out against "following" and "emerging" organizations and help them achieve and even exceed business goals? The research indicates that "leading" organizations excel in key areas, including:

Aligning security strategies with critical business assets. "Leading" organizations know all about the assets on their network, and so they are also more likely to understand the business impact of threats and vulnerabilities. This level of visibility and knowledge can help "leading" organizations bolster protection on critical business assets and prioritize incident response actions upon threat detection (see Figure 5). "Leading" organizations follow a similar strategy of correlating threat intelligence with critical business assets by focusing threat intelligence analysis on cyber-adversaries, campaigns, and the tactics, techniques, and procedures (TTPs) used in targeted attacks on the organization, industry, geography, etc. This threat intelligence analysis is then carefully compared to things like access patterns for critical applications, file distribution to executives, or "typosquatting" domains used to emulate an organization's website in phishing campaigns. "Leading" organizations may also use threat intelligence analysis in threat hunting processes for retrospective investigations. In this way, "leading" organizations can more effectively identify risks as described in the NIST CSF.

Figure 5: The Business's Perception of the Security Team, by Cybersecurity Maturity

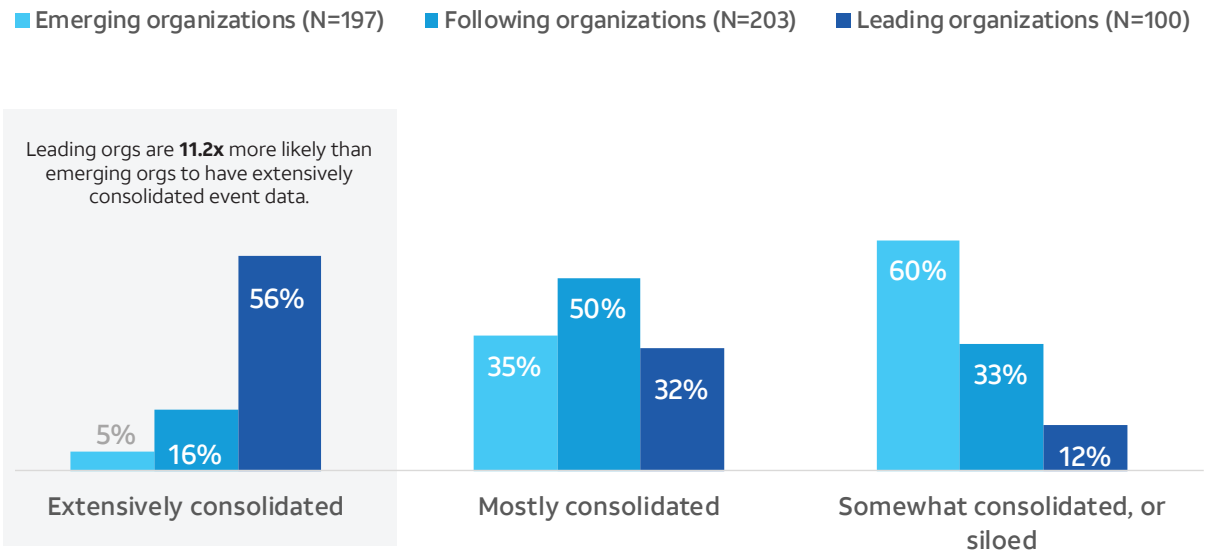
How effective is your organization at using its understanding of the business impact of threats and vulnerabilities to prioritize incidents in which to respond? (Percent of respondents)



Consolidating and addressing security event data. More than half of "leading" organizations (56%) claim that their security event data (from networks, endpoints, cloud-based workloads, threat intelligence feeds, etc.) is "extensively consolidated" (see Figure 6). This means that they are collecting and processing real-time and historical security telemetry in a consistent way using a common data pipeline and data management infrastructure (i.e., log management, SIEM, data lake, etc.). Consolidated security data can then be provided to various security analytics engines for threat detection and cyber-risk monitoring.

Figure 6: Event Environment and Investigation, by Cybersecurity Maturity

Generally speaking, how would you describe your organization's event data? (Percent of respondents)

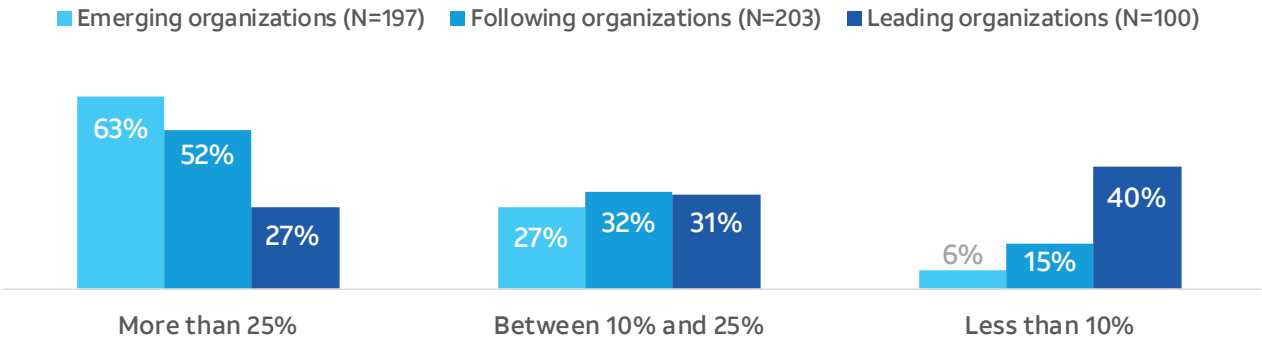


By consolidating security event data, "leading" organizations tend to generate more security events and alerts than "following" or "emerging" organizations on a monthly basis. Nevertheless, "leading" organizations are not overwhelmed by monthly "alert storms." In fact, the data suggests just the opposite. A good percentage (40%) of "leading" organizations claim that their security team ignores less than 10% of security events/alerts per month even though it might be worthwhile to investigate them (see Figure 7).

In truth, the data demonstrates that even "leading" organizations are not perfect. Despite their attention to detail, they are not able to triage, investigate, or prioritize all security events/alerts. Nevertheless, 40% of "leading" organizations can successfully address about 90% of security events/alerts on a monthly basis. Aside from consolidating their security data, "leading" organizations likely have developed playbooks for event/alert treatment delegating work to multiple tiers of SOC analysts. It's also likely that "leading" organizations use process automation, assigning prosaic tasks to machines rather than humans. Finally, "leading" organizations probably have an orchestrated process for security event/alert management tied directly into security controls for mitigation actions (i.e., quarantining a system, changing a rule, sending an email to IT operations, etc.).

Figure 7: Event Environment and Investigation, by Cybersecurity Maturity

What percentage of the overall volume of security events/alerts do you believe your organization ignores, even though it would be beneficial to investigate, because it is impractical to investigate every alert? (Percent of respondents)

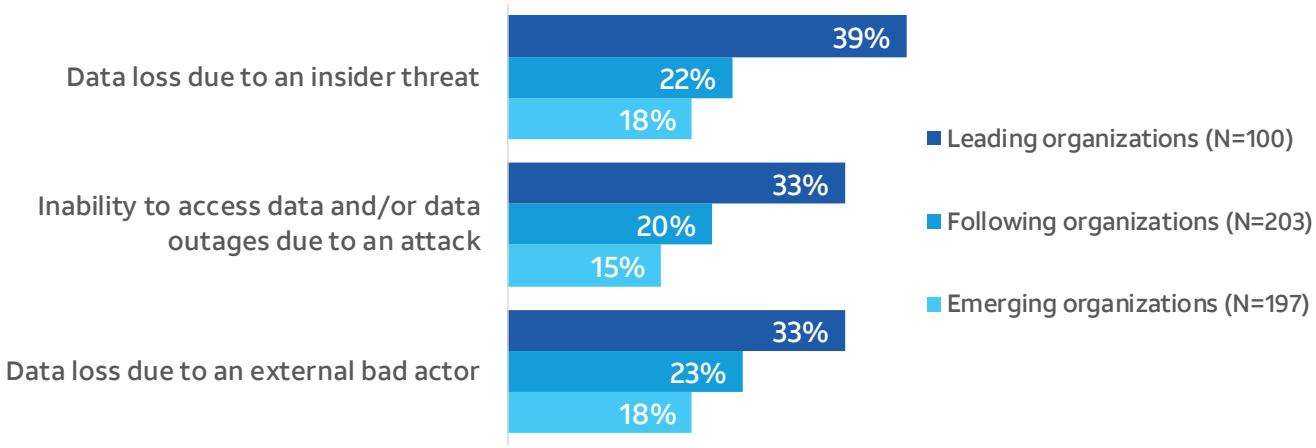


Based on this, data leading orgs. investigate **~1,190** more security events per month, relative to emerging orgs (on average).

While "leading" organizations seem to be better at security event management, does this actually improve threat prevention? The data suggests it does. Over the past 12 months, 39% of "leading" organizations have not experienced data loss due to an insider threat, compared to 22% of "following" organizations and 18% of "emerging" organizations, in short "leading" organizations have experienced less data loss. Similarly, 33% of "leading" organizations have not experienced a security incident resulting in the inability to access data or data outages due to a cyberattack (compared to 20% of "following" organizations and 15% of "emerging" organizations), and 33% of "leading" organizations have not experienced data loss due to an external bad actor (compared to 23% of "following" organizations and 18% of "emerging" organizations, see Figure 8).

Figure 8: Percent of Organizations Experiencing Incidents in the Last 12 Months, by Cybersecurity Maturity

In the last 12 months, approximately how many of the following security incidents has your organization experienced due to the following threats? (Percent of respondents reporting "None")



"Leading" organizations have a big advantage, as 82% are very effective with incident response and 84% are very effective with recovery.

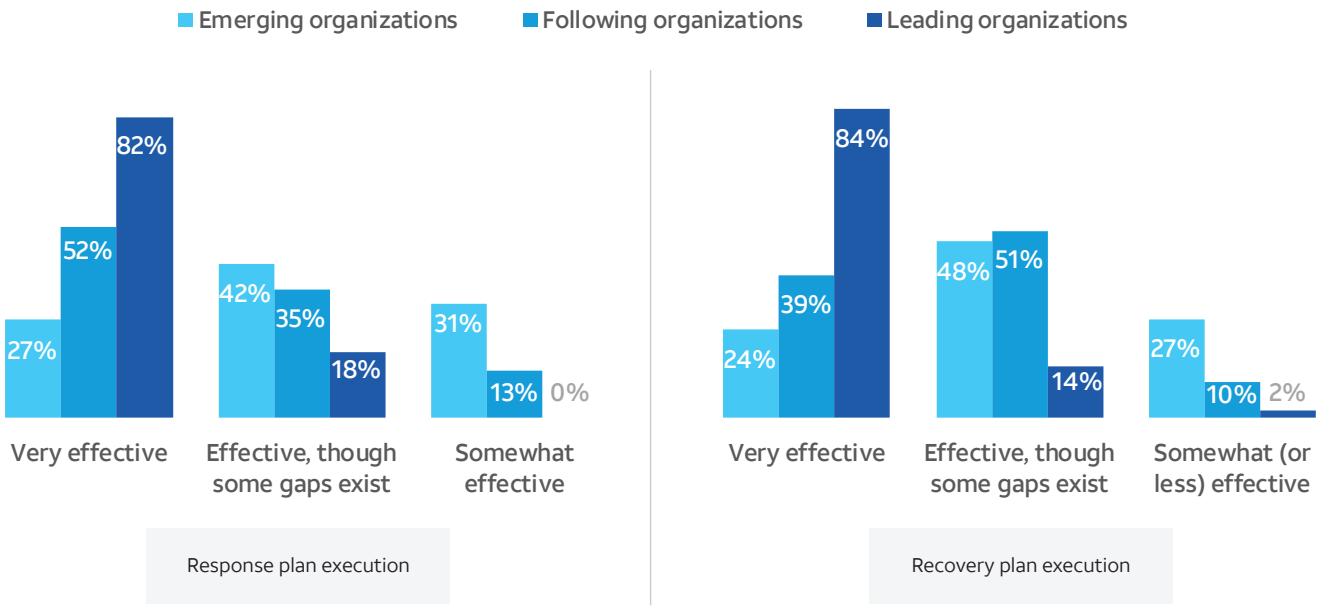
While this data demonstrates superior performance by "leading" organizations, it is worth noting once again that most are still impacted by all three types of threats described in figure 8. Indeed, two-thirds of "leading" organizations have experienced a security incident resulting in the inability to access data or in a data outage due to a cyberattack and the same can be said about incidents leading to data loss due to an external bad actor. A determined and sophisticated cyber adversary can usually figure out ways to penetrate the defenses of even the most prepared organization.

"Leading" organizations understand this and continue to excel once a system is compromised. In fact, "leading" organizations have a big advantage, as 82% are very effective with incident response and 84% are very effective with recovery (see Figure 9).

ESG believes that strong recovery scores are related to years of business continuity/disaster recovery (BC/DR) experience, likely honed through years of experience in disaster response (i.e., 9/11, hurricanes, wildfires, etc.) and regulatory compliance. This knowledge is especially important given how 2020 events have challenged business continuity.

Figure 9: Response and Recovery Execution, by Cybersecurity Maturity

How effective is your organization at executing its response and recovery plans during or after an incident? (Percent of respondents)



As for incident response (IR), ESG believes that "leading" organizations excel for several reasons:

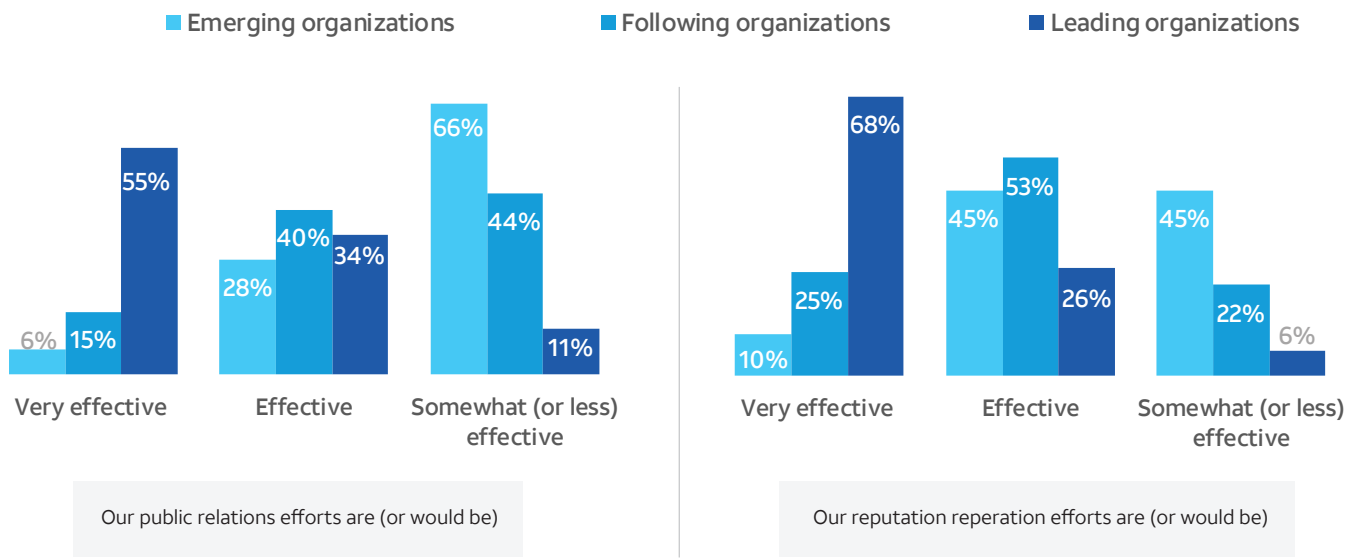
IR plans are well documented and tested. "Leading" organizations attend to all the details by documenting the IR plan from start to finish. Once a security incident is escalated, the IR plan commences, and all participants know what to do. To gain actual experience, "leading" organizations also tend to test their IR plans with tabletop exercises, red teaming, or war gaming. This can help them expose and fine-tune areas of weakness or address unexpected issues.

"Leading" organizations seek help. Crafting and executing an IR plan requires experience and esoteric skills, so "leading" organizations often pursue help from service providers with IR expertise.

IR programs span beyond technology. "Leading" organizations define roles and responsibilities across the organization. Business leaders are involved in contingency planning, legal teams have a plan for working with compliance auditors, public relations (PR) personnel are prepared to speak with the press, and the organization has a formalized communications plan that ensures all internal and external stakeholders are appropriately informed.

IR planning, testing, and continuous improvement can help organizations diminish the impact of a security incident and accelerate business operations recovery. For example, the research indicates that "leading" organizations are very effective in dealing with PR and brand reputation aspects of IR (see Figure 10). This reinforces the fact that IR is treated as a business, not just a technical process where the entire team has clear roles and responsibilities (i.e., for executives, legal, human resources, PR, etc.), and follows defined playbooks, test and practice plans, etc.

Figure 10: Ability to Limit Damage to the Brand due to an Incident, by Cybersecurity Maturity



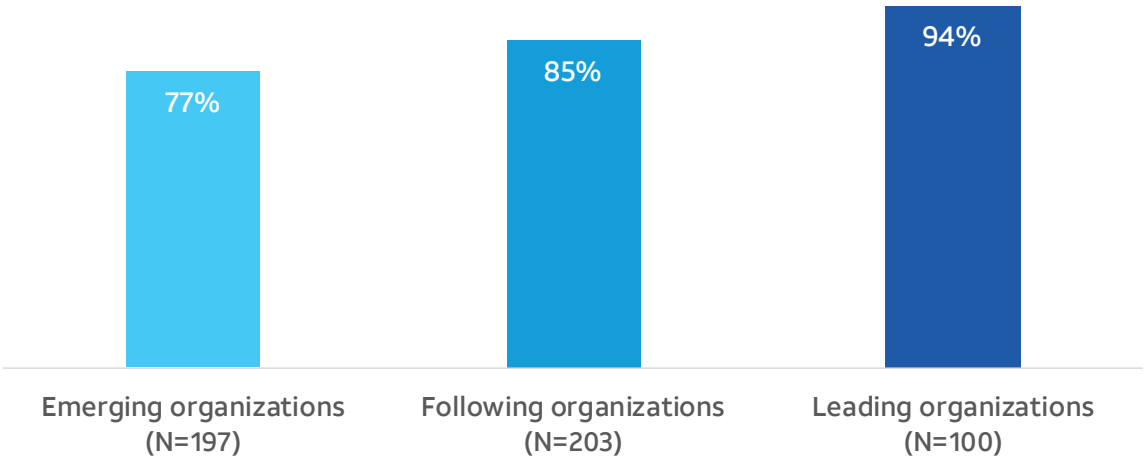
Cybersecurity can be difficult, as it requires continuous improvement and advanced skills. "Leading" organizations understand that meeting challenges and goals may be beyond the ability of the internal staff alone. Therefore, 94% use a managed service provider for some aspects of cybersecurity. Often, services are used to offload pedestrian tasks or provide help in areas requiring cutting-edge experience and skills (see Figure 11).

In this way, service providers act as a force multiplier for "leading" organizations by extending the staff skills and capacity.

94% of "leading" organizations use a managed service provider for some aspects of cybersecurity.

Figure 11: Tendency of Organizations to Utilize MSPs, by Cybersecurity Maturity

Does your organization use a managed service provider to operate any aspect of its cybersecurity/information security environment? (Percent of respondents indicating they do)



Keys to success

Strong cybersecurity requires constant training, process improvement, and continuing investment. To reinforce this closed-loop process, the NIST CSF uses a four-tier taxonomy (Partial, Risk-informed, Repeatable, Adaptable) that CISOs can use to assess their current and target profile—where they are and where they want to be. For example, a mature organization may have repeatable processes for security activities like vulnerability management. This would be their current profile per the NIST CSF. This same organization may seek to improve its vulnerability management program by using machine learning algorithms to compare software vulnerabilities to known exploits and adversary attack patterns on a continual basis. This target profile would align with the NIST CSF "adaptable" tier.

The data shows that "leading" organizations' behavior exemplifies a commitment to continuous cybersecurity improvement. For example, "leading" organizations have made great advances in their cybersecurity posture over the past 2 years (see Figure 12). It is likely that they have moved along the maturity continuum, making improvements in all five NIST CSF functions.

Figure 12: Momentum Improving Security Posture over Time, by Cybersecurity Maturity

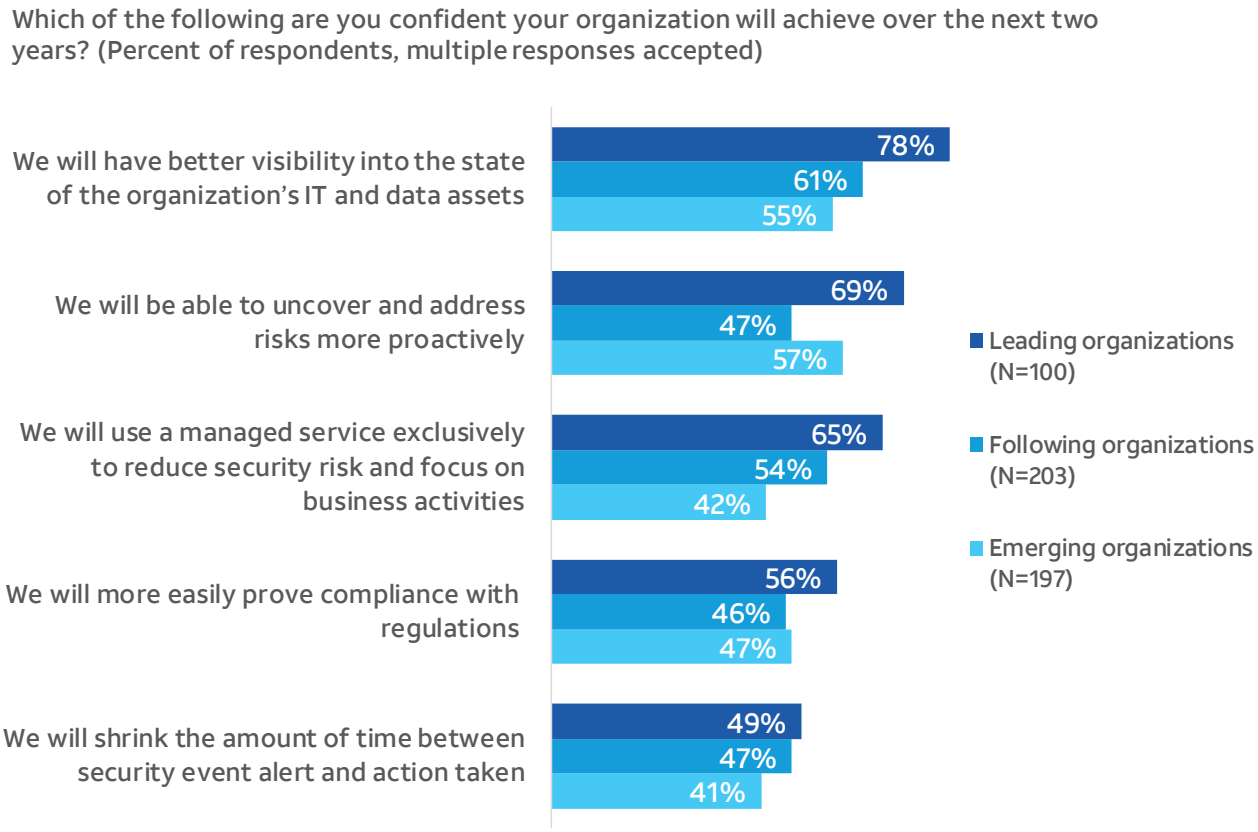
To the best of your ability, please indicate the level of improvement of your organization's cybersecurity posture compared to two years ago. (Percent of respondents)

Achieving greater visibility into the state of the organization's IT and data assets could represent an evolution from the repeatable to the adaptable tier.

"Leading" organizations tend to identify areas for improvement like gaining more detailed visibility, proactively uncovering/mitigating cyber risks, and finding areas to work with service providers (see Figure 13). Consequently, they are willing to increase cybersecurity budgets more aggressively (see Figure 14).

This data may illustrate a progression along the NIST CSF functions. For example, achieving greater visibility into the state of the organization's IT and data assets could represent an evolution from the repeatable to the adaptable tier. The repeatable tier is highlighted by a formal, documented, and adopted risk management processes. The repeatable tier is then enhanced by adding strong data analytics to provide insights which can be used to fine-tune controls, mitigation actions, and policies. "Leading" organizations are likely increasing data collection, processing, and analytics in pursuit of this type of advancement.

Figure 13: How Respondents Think Security Preparedness Will Change, by Cybersecurity Maturity

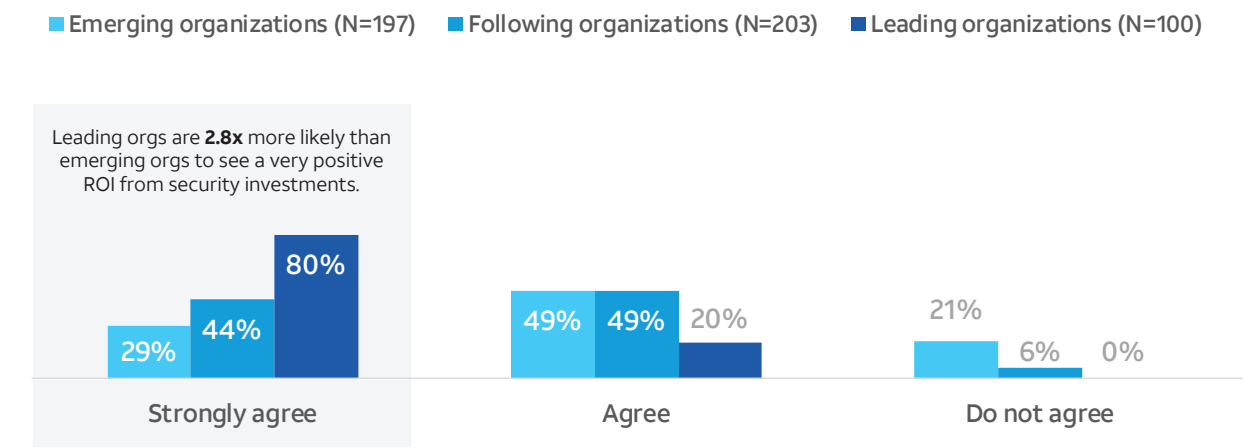


"Leading" organizations also know the attack surface and how it's changing with the addition of digital transformation applications, IoT device adoption, and work-from-home (WHF) initiatives. As previously mentioned, CISOs at "leading" organizations are also aware of their strengths and weaknesses. "Leading" organizations also understand their position on the NIST CSF framework—their current and target profile.

Figure 14: How Respondents Think Security Preparedness Will Change, by Cybersecurity Maturity

Armed with this knowledge and a thorough assessment of their cybersecurity requirements, "leading" organizations may be more likely to make strategic rather than tactical investments in cybersecurity. In other words, cybersecurity investments are targeted to address existing gaps or support new business initiatives. Furthermore, "leading" organizations may have progressed to the "adaptable" tier of the NIST CSF, where policies and controls are changed based upon lessons learned and data analysis. This may explain why 100% of "leading" organizations strongly agree or agree that ROI on time and investments in their security organization and controls is very positive (see Figure 15).

Figure 15: ROI on Security Investments, by Cybersecurity Maturity



Conclusions

Since its introduction in 2014, the NIST CSF has gained popularity and is now used as a global standard to help organizations identify and mitigate cyber-risk while providing a roadmap for cybersecurity program improvement. Additionally, the NIST CSF is universally valuable as it is designed for use by organizations of all sizes.

In assessing the data from this research project, ESG believes there is still work ahead across all five functions of the NIST CSF. Specifically:

Organizations must identify risks across the changing attack surface. IT is changing as organizations adopt SaaS applications, move workloads to the public cloud, and embrace new digital transformation applications. The pace of change will only increase in the future as 5G proliferates. This means risk identification and mitigation must become a dynamic process based upon a real-time understanding of the IT environment and threat intelligence. To keep up, organizations must pursue an aggressive strategy to reach the "adaptable" tier of the NIST CSF.

Incident prevention must be based on a feedback loop. While prevention techniques like anti-virus (AV) signatures and firewall rules will always be required, static defenses must be supported with dynamic controls that fine-tune threat prevention based upon environmental factors like network traffic patterns, user locations, and changing threat actor campaigns.

Threat detection must be aligned with business context and event consolidation. Monitoring all traffic, sensitive data access, and user behavior is beyond the scale of most cybersecurity teams. To cope with this reality, organizations must focus their efforts on event consolidation—especially for business-critical individuals, applications, and data. The data presented in this report demonstrates that "leading" organizations are already pursuing these types of strategies.

Incident response planning really matters. IR requires a systemic approach across an organization, which can be difficult to create and manage. The only way to address these difficulties is with collaboration, communication, and planning across the organization. Successful IR teams include active CEOs and other department heads, willing to put in the work, test their plans, and strive for continuous improvement.

Recovery must incorporate new scenarios. As previously mentioned, recovery plans are often mature, based on years of business continuity and disaster recovery (BC/DR) requirements. A good start, but organizations have learned recently that they must continuously broaden their perspective to consider recovery operations in new types of scenarios like global pandemics.

Strong cybersecurity is a perpetual journey with no destination, so it is no surprise that organizations have more work to do across the five NIST CSF tiers. This is one reason why leading organizations work together with service providers, providing guidance along the way.

Finally, the research also demonstrates that there is a relationship between strong security and business achievement. To be clear, security does not beget business success, but the data presented in this report suggests that successful organizations are willing to invest in security and build a bridge between cybersecurity and business mission and goals. Based upon this research project, this commitment to strong security can lead to business benefit.

Appendix I: research methodology and demographics

To gather data for this report, AT&T Cybersecurity commissioned ESG to conduct a comprehensive survey of cybersecurity and IT professionals with significant influence over their organization's purchase process for cybersecurity technology investments. All respondents were located in North America and employed at organizations with at least 500 employees and annual revenues of $50 million USD or more. The survey was fielded between January 30, 2020 and March 2, 2020. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on several criteria) for data integrity, a final sample of 500 respondents remained. Figures 16-20 detail the demographics of the respondent base, including their role and responsibility areas. Firmographics include organizations' total number of employees, primary industry, and annual revenues. Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

Figure 16: Respondents by Role

Which of the following best (i.e., most closely) describes your current position within your organization? (Percent of respondents, N=500)

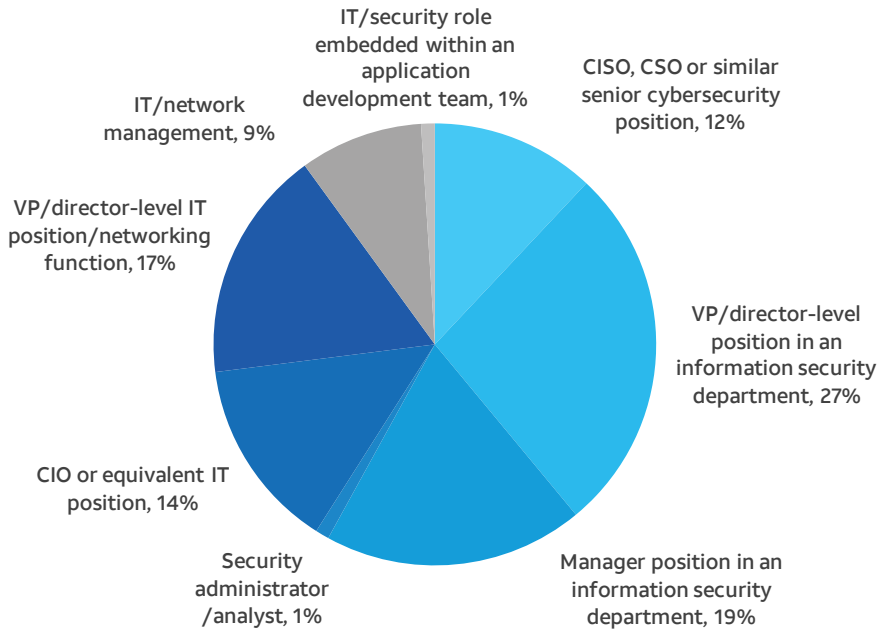


Figure 17: Respondents' Security Responsibilities

Which areas of cybersecurity are you most responsible for daily? (Percent of respondents, N=500, three responses accepted)

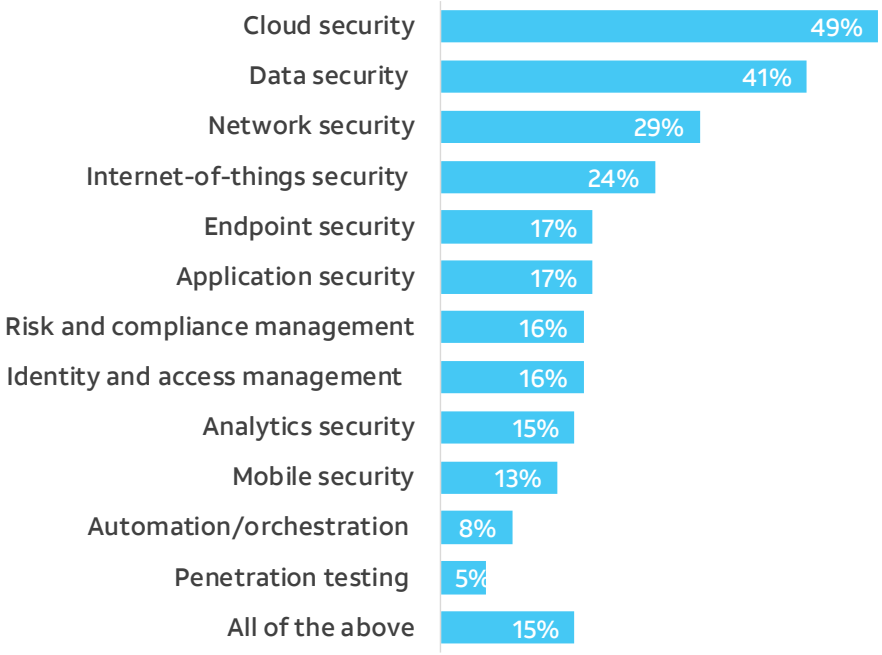


Figure 18: Respondents by Company Size (Number of Employees)

How many total employees does your organization have worldwide? (Percent of respondents, N=500)

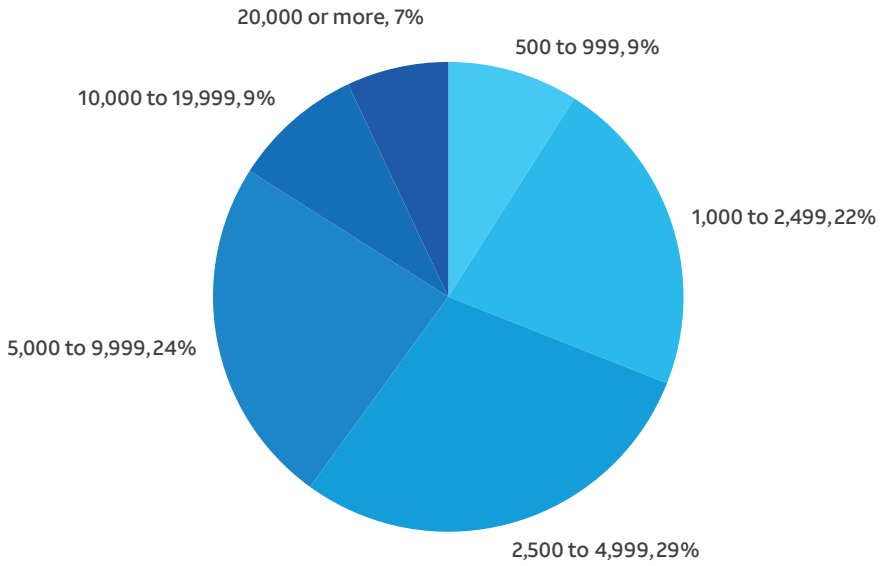


Figure 19: Respondents by Company Size (Annual Revenue)

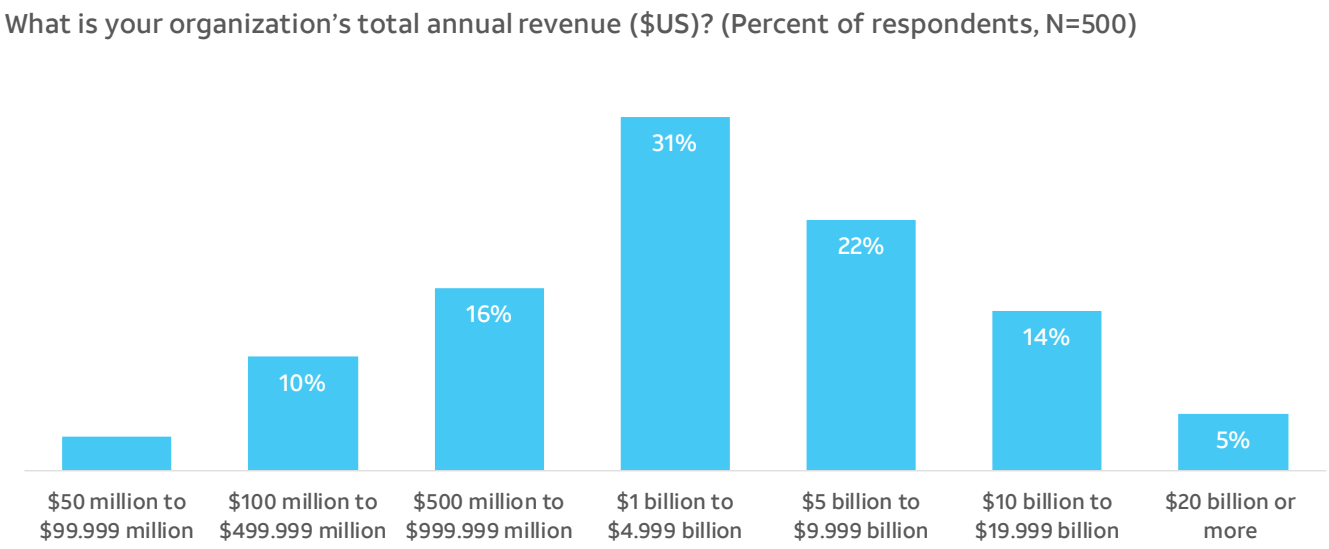
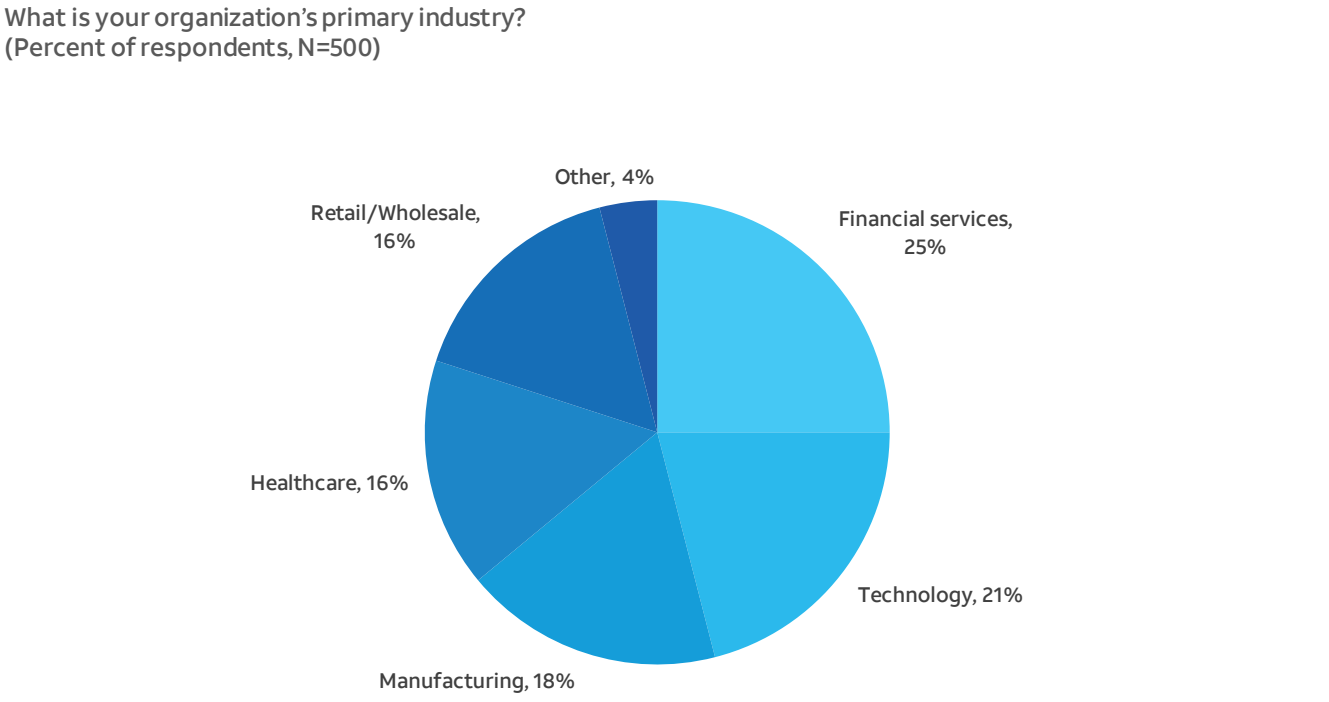


Figure 20: Industries Represented



Appendix II: established levels of cybersecurity maturity used in this report

To segment organizations by their cybersecurity maturity, AT&T Cybersecurity and ESG considered each respondent's response to 16 questions directly relatable to principles and best practices prescribed by the NIST CSF. Based on the answers to these and other questions, respondents' organizations could earn between 0 and 100 maturity points. The organizations represented by the lowest scoring 39% of respondents were placed in the least mature "emerging" category, organizations in the middle of the pack were placed in the "following" category, and those that comprised the top 20% of scores were placed in the "leading" category.

Figures 21-35 outline the scoring questions ESG asked respondents, the overall distribution of responses, and the maturity points earned with each response.

Figure 21: Cybersecurity Program Formalization

In general, how would you describe your organization's internal cybersecurity program and policies? (Percent of respondents, N=500)

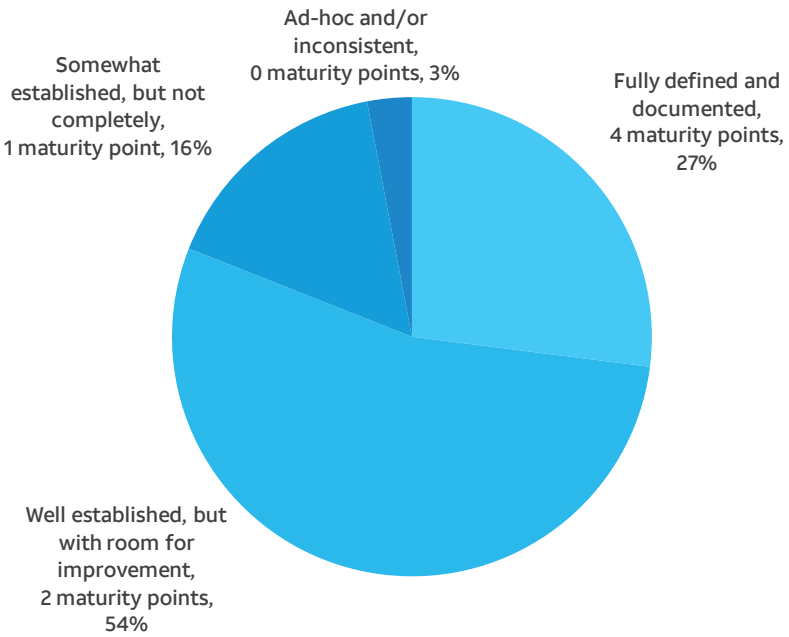


Figure 22: Extent of Asset Inventorying

To what extent has your organization inventoried and prioritized (based upon classification, criticality, and business value) each of the following? (Percent of respondents, N=500)

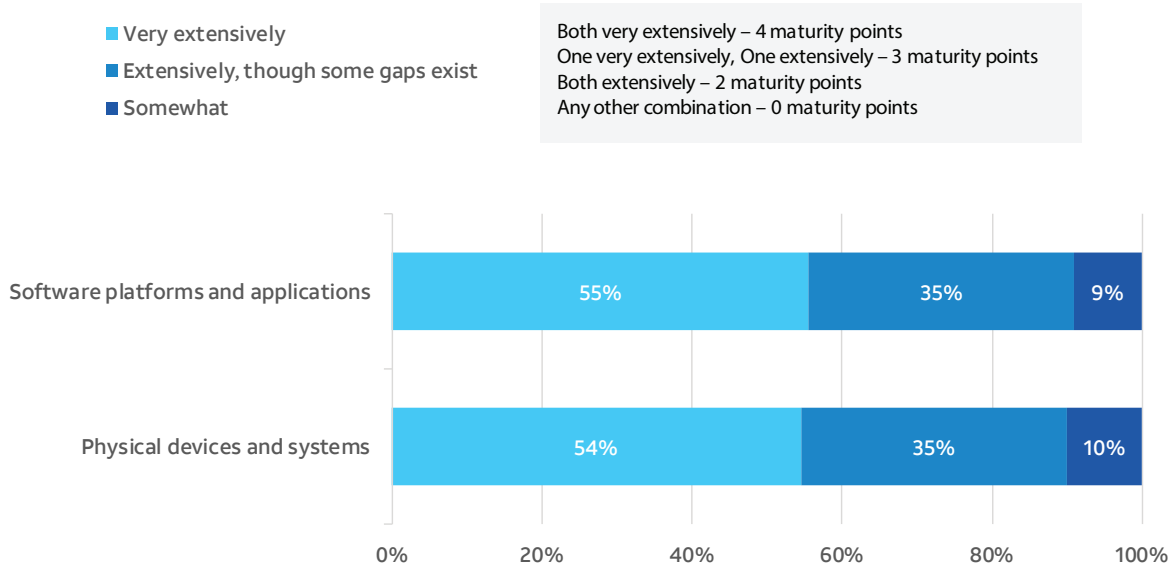


Figure 23: External Threat Identification

To what extent would you say your company has identified and documented the business impact of external vulnerabilities and threats? (Percent of respondents, N=500)

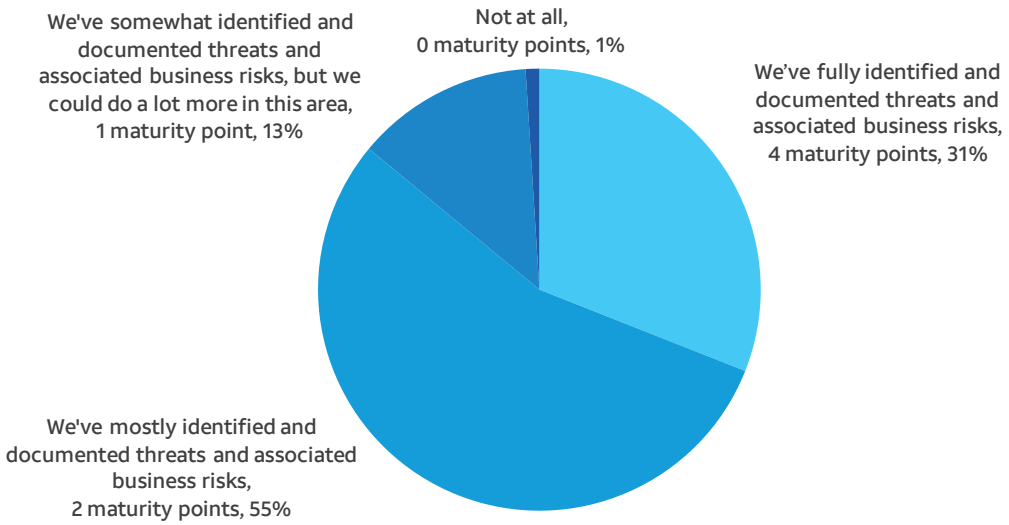


Figure 24: Internal Threat Identification

To what extent would you say your company has identified and documented the business impact of internal vulnerabilities and threats? (Percent of respondents, N=500)

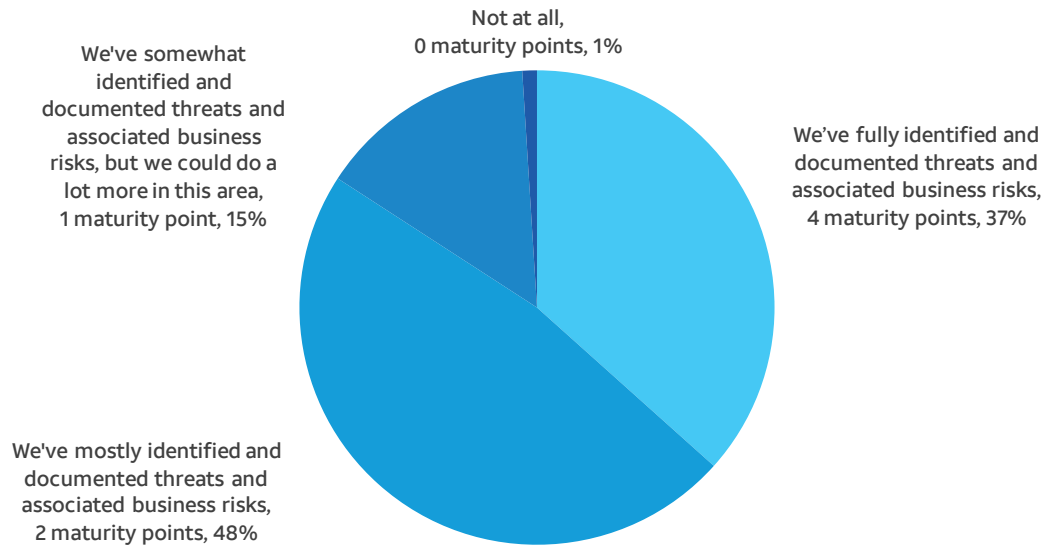


Figure 25: Frequency with which Organizations Review CSF 'Identification' Areas

How often are established processes/documentation in each of the following areas formally reviewed/revised based on changing requirements and security trends? (Percent of respondents)

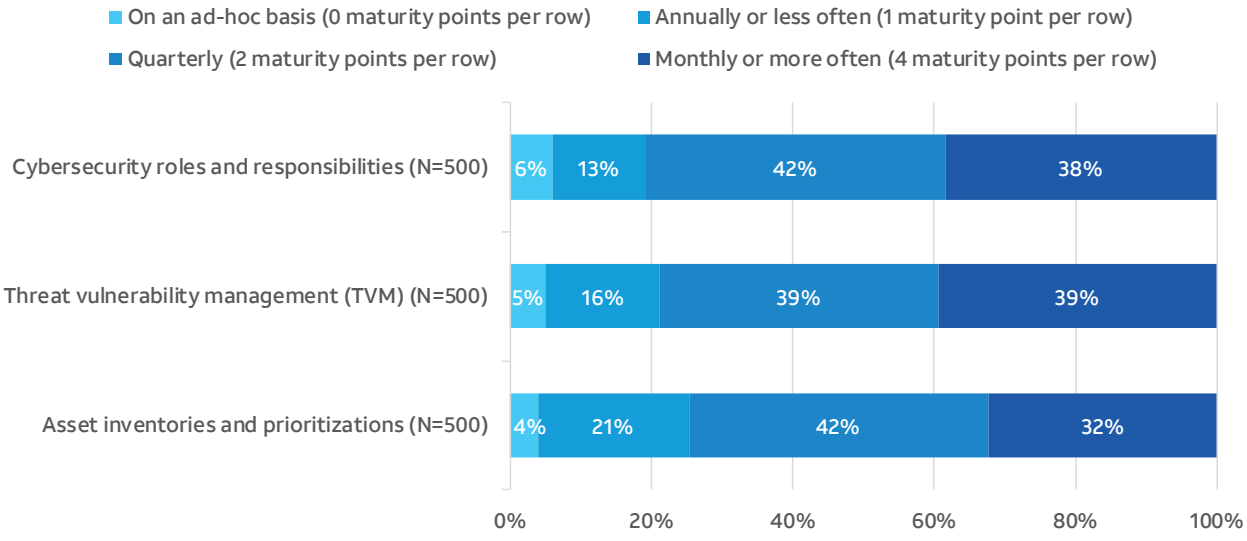


Figure 26: Ability to Limit Employee Access

How effective is your organization at tightly controlling and managing employee access to business systems and data according to the principles of least privilege? (Percent of respondents, N=500)

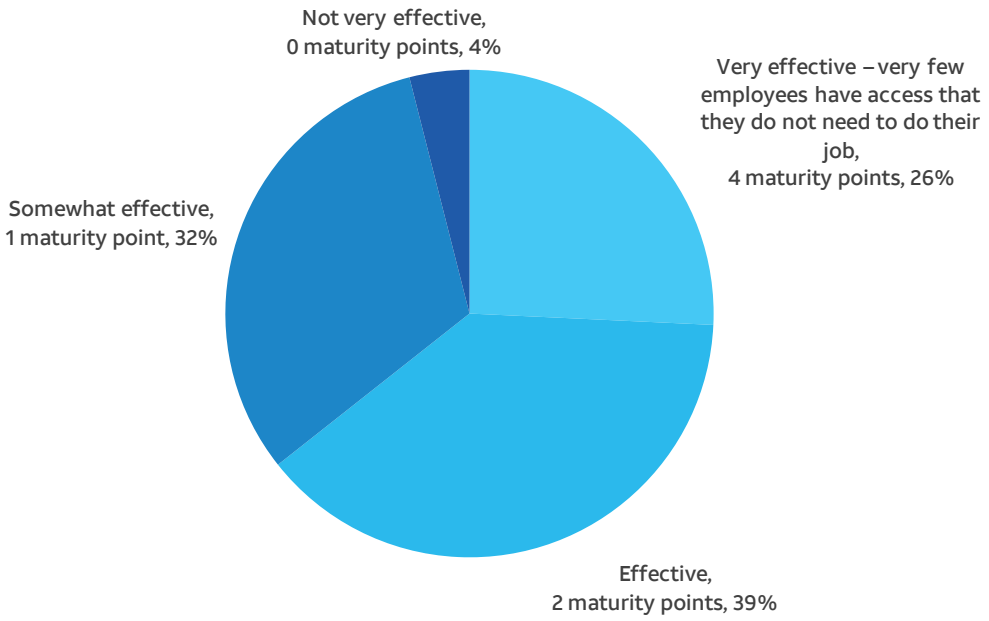


Figure 27: Ability to Properly Configure System Access

To what extent has your organization incorporated the concept of "no unnecessary services" into its IT systems' security configuration policies? (Percent of respondents, N=500)

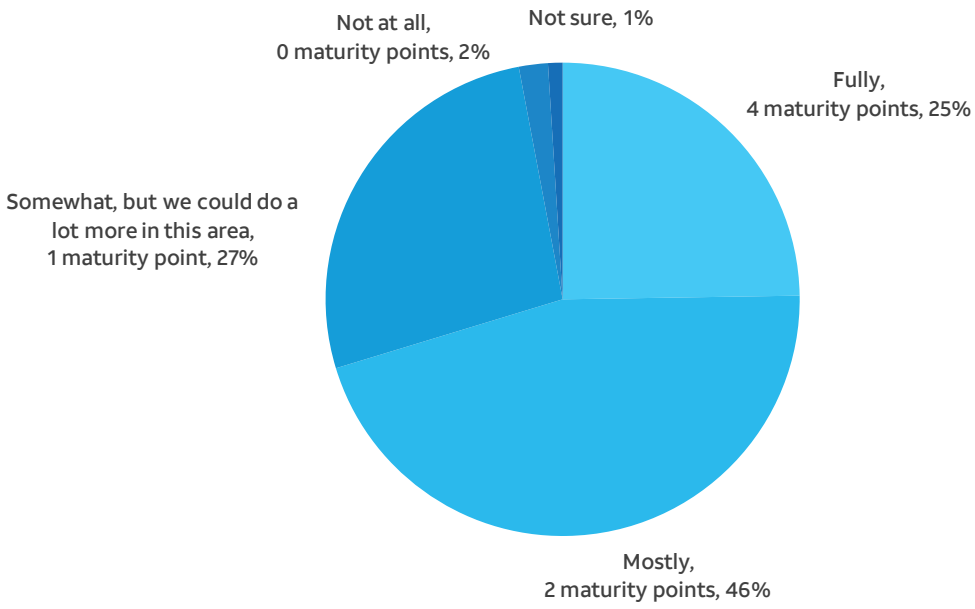


Figure 28: Data Encryption Due Diligence

To what extent does your organization consider data classification, sensitivity, and regulatory requirements when deciding if data needs to be encrypted? (Percent of respondents, N=500)

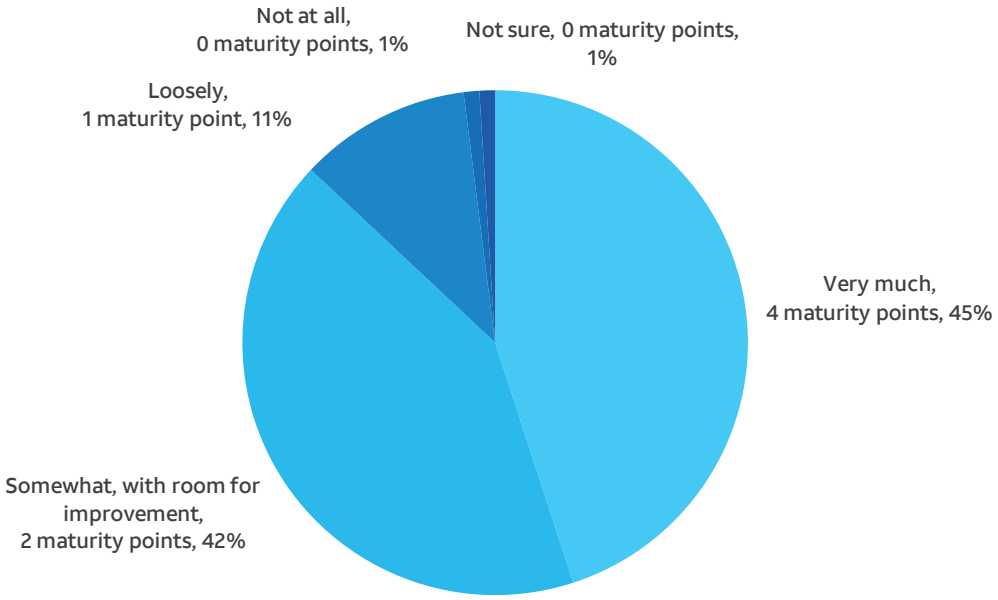


Figure 29: Extent of Network Segmentation

Does your organization segregate/segment its networked business systems and data? (Percent of respondents, N=500)

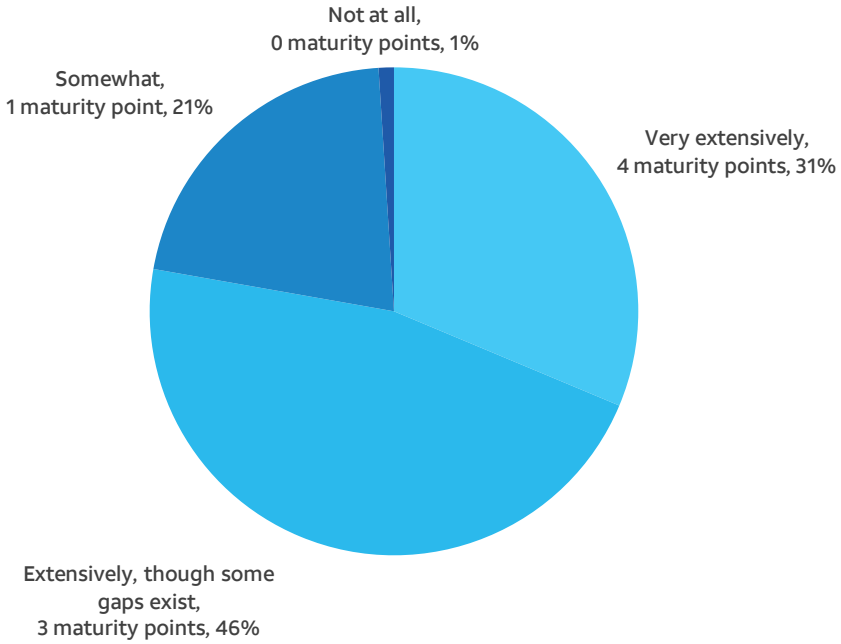


Figure 30: Frequency of Cybersecurity Training, by Role

What best describes the frequency with which your organization conducts formal cybersecurity awareness education/training for its personnel? (Percent of respondents, N=500)

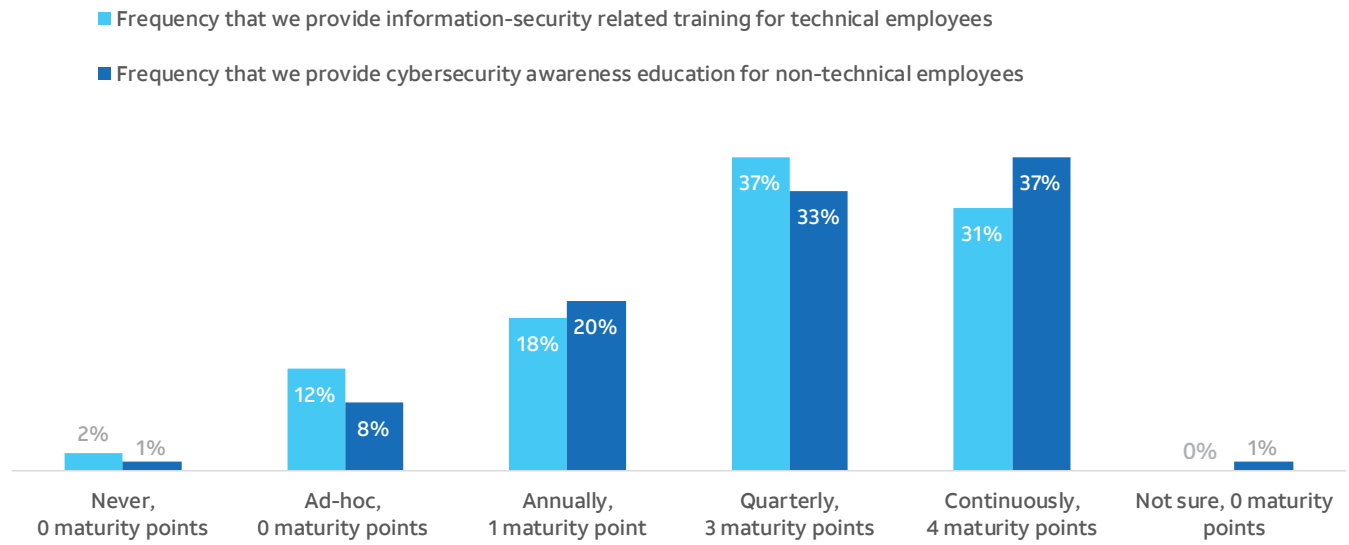


Figure 31: Frequency with which Organizations Review CSF 'Protection' Areas

How often are established processes/controls/documentation in each of the following areas formally reviewed/revised based on changing requirements and security trends? (Percent of respondents)

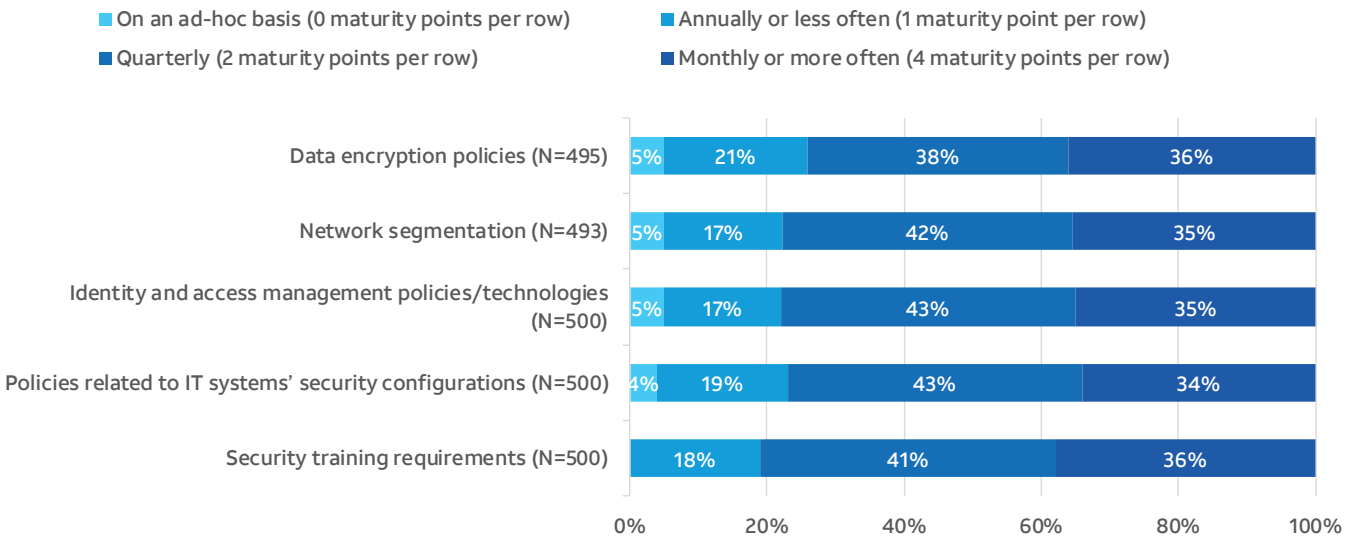


Figure 32: Use of Threat Intelligence within SIEM

How does your organization leverage threat intelligence capabilities within a security incident and event management (SIEM) solution? (Percent of respondents, N=487)

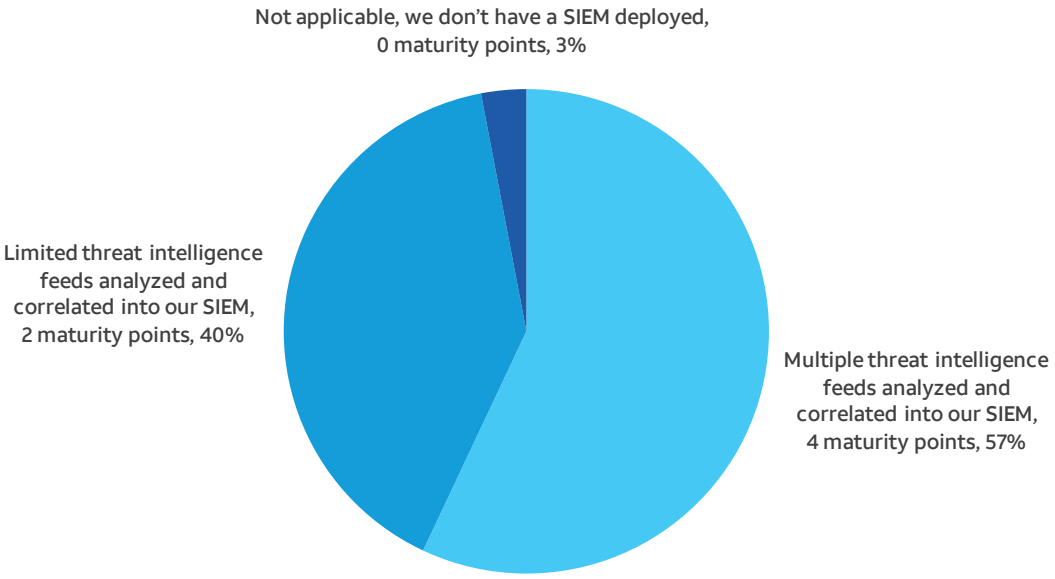


Figure 33: Staffing for Event Detection

To what extent has your company defined roles and responsibilities for event detection? (Percent of respondents, N=500)

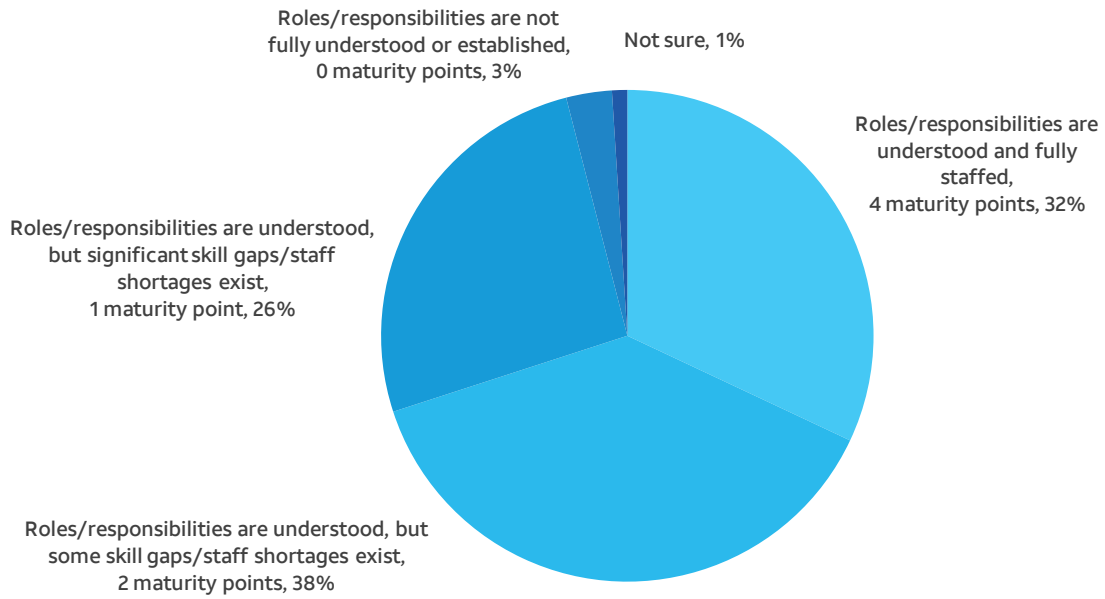


Figure 34: Incident Communication

When a security incident is discovered, what best describes the process for communicating details to relevant stakeholders? (Percent of respondents, N=500)

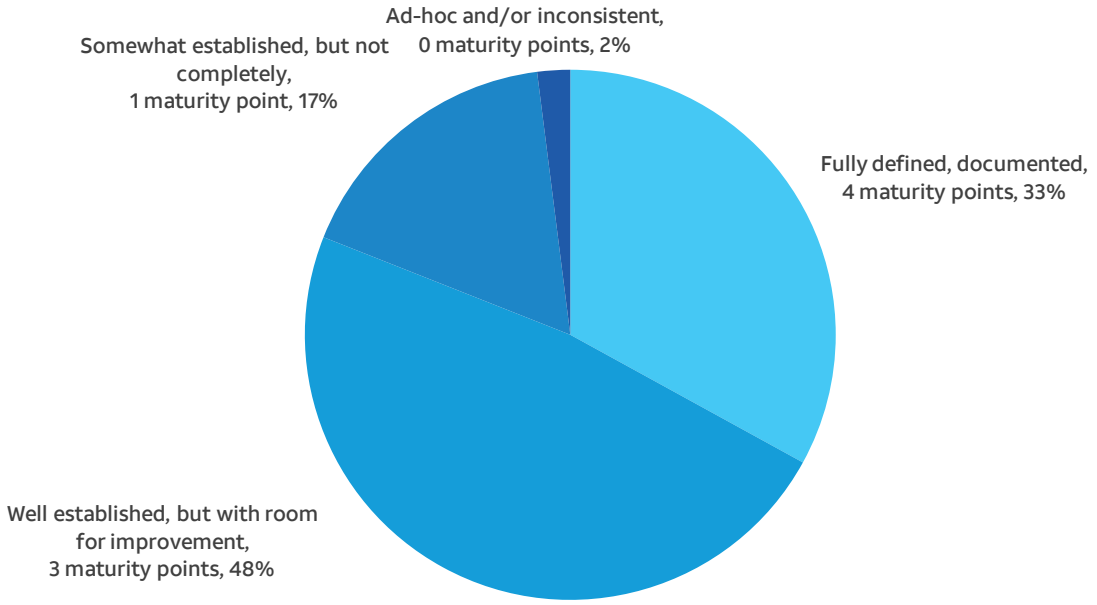
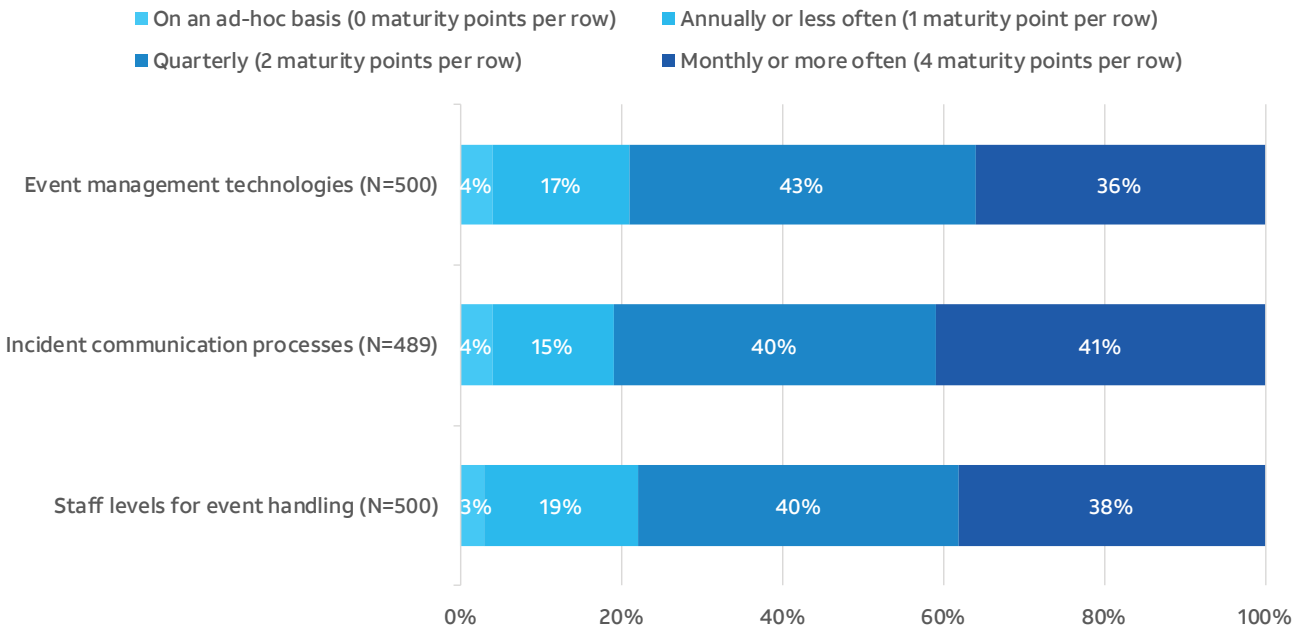


Figure 35: Frequency with which Organizations Review CSF 'Detection' Areas

How often are established processes/controls/documentation in each of the following areas formally reviewed/revised based on changing requirements and security trends? (Percent of respondents)



About AT&T Cybersecurity

AT&T Cybersecurity helps to reduce the complexity and cost of fighting cybercrime. Together, the power of the AT&T network, our SaaS-based solutions with advanced technologies including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange™, and our relationship with more than 40 best-of-breed vendors, all accelerate your response to cybersecurity threats. Our experienced consultants and SOC analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.

www.cybersecurity.att.com

Online Maturity Assessment

AT&T Cybersecurity and ESG have developed a free self-assessment survey for measuring an organization's security maturity, based on the benchmark data from this study and the NIST cybersecurity framework. To take the assessment and receive a customized maturity report, go to:
AT&T Cybersecurity maturity assessment survey.

About ESG

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

AT&T Business