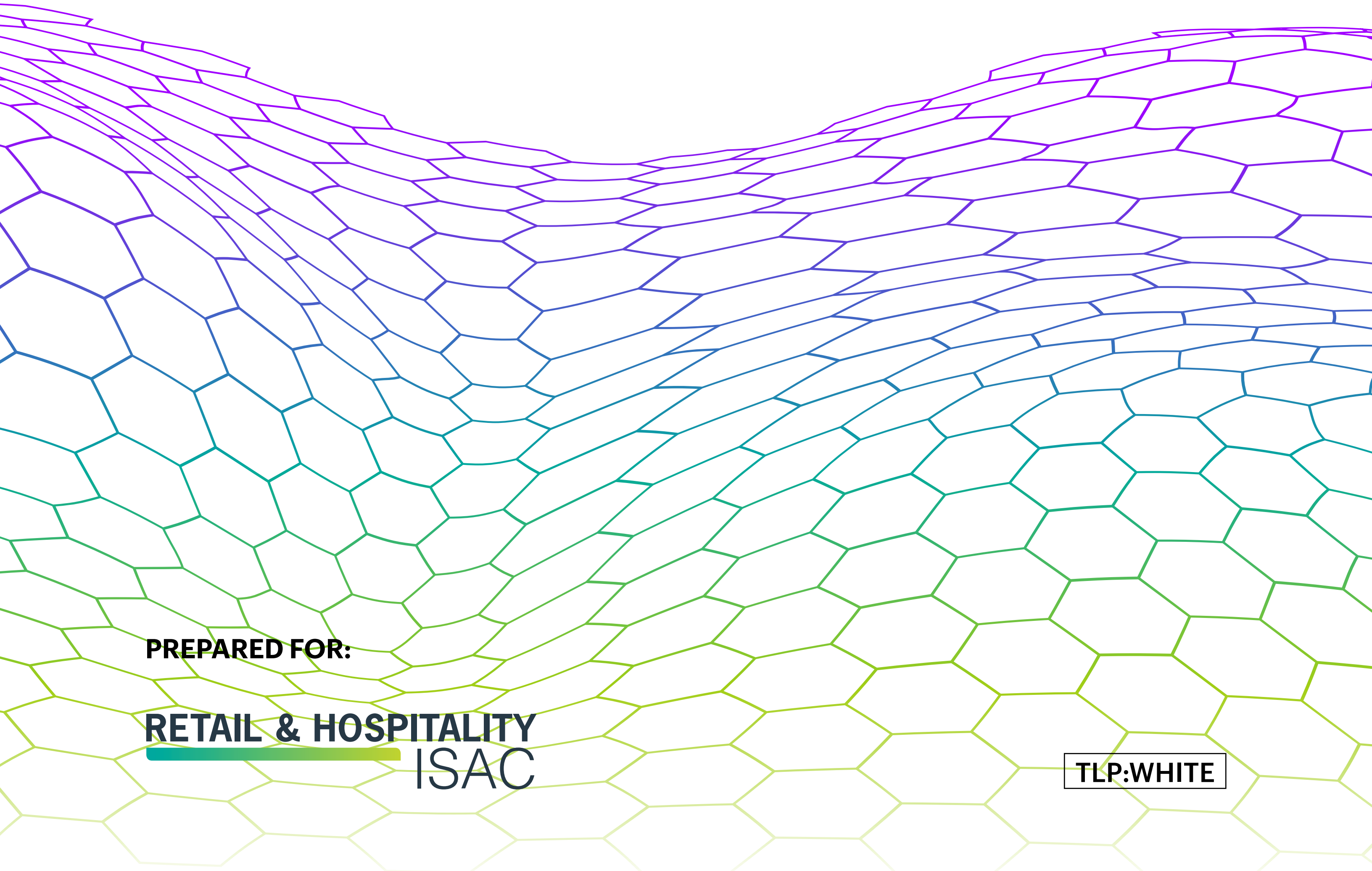
accenture

BUILDING THE FOUNDATION OF YOUR CYBERSECURITY PROGRAM

WHERE TO START AND HOW TO GROW



PREPARED FOR:

RETAIL & HOSPITALITY ISAC

TLP:WHITE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Retail & Hospitality Information Sharing and Analysis Center (RH-ISAC) is the trusted community for sharing sector-specific cyber security information and intelligence.

The RH-ISAC connects information security teams at the strategic, operational and tactical levels to work together on issues and challenges, to share practices and insights, and to benchmark among each other—all with the goal of building better security for the retail and hospitality industries through collaboration. RH-ISAC serves all retail and hospitality companies, including physical and online-only retailers, restaurants, hotels, gaming casinos, food retailers, consumer products and more. For more information, visit www.rhisac.org.

Building the Foundation of Your Cybersecurity Program is a guide that was developed by Accenture with member support from the RH-ISAC Security Operations Working Group.

The mission of the RH-ISAC Security Operations Working Group is to foster a collaborative forum to share best practices on how resource-strapped teams can maximize resources—including those provided by the RH-ISAC—to strengthen their defenses and be better able to communicate their position and future needs with internal stakeholders.

The cybersecurity landscape is continuously evolving, and organizations need to take steps to protect themselves from increasingly complex threats on an ongoing basis. This means investing in, building, and maintaining an appropriate cybersecurity program to protect enterprise assets as well as customer data. Building a strong cybersecurity program requires a multifaceted approach that combines diverse skill sets, processes, tools and technology. Usually, oversight is another integral piece of the puzzle, both from internal and external entities. This guide focuses on aiding organizations in determining if they possess the appropriate people, process, technology, and oversight to operate an effective cybersecurity program.

TLP:WHITE

PEOPLE – SKILLSETS AND KNOWLEDGE

Cybersecurity professionals are on the front lines of protecting the organization’s “crown jewels” and it is important to enlist team members with the right skill sets to run a successful cybersecurity program.

Cybersecurity professionals are in high demand and short supply, and this trend will continue. According to Gartner TalentNeuron, there was anticipated talent shortage of nearly 2 million jobs by end of 2019. The global COVID-19 pandemic has resulted in a surge in demand for cybersecurity professionals, with a 65% upswing in demand in the U.S. alone.[1] This shortage creates a challenge for organizations, as it means they need to show a competitive advantage to attract and retain the best talent, ensure they are filling the required skill sets, and get the most out of their current people with the processes and technologies they have in place.

In this sub-section, we provide insights on how organizations should structure their cybersecurity program functions to maximize effectiveness of the available resources, so they can provide adequate coverage for all aspects of cybersecurity. We will review the following four key areas:

i. Cybersecurity program functions

ii. Headcount and expertise requirements

iii. Tools for evaluating existing cybersecurity staff

iv. Cybersecurity employment and attracting talent

Cybersecurity program functions

Cybersecurity programs should make every effort to provide capabilities across key functions that help an organization manage the entire lifecycle of cybersecurity controls. Aligning the organization's resources in specific functions helps to focus available resources, maximize their effectiveness, and ensure availability of skills to meet their cybersecurity goals.

A successful way to group teams into functions is to align the resources per the NIST Cybersecurity Framework (NIST CSF).[2] As discussed in Section 1 above, the NIST CSF identifies the following five primary functions for a cybersecurity program and these functions could be used to structure cybersecurity teams:

- **Identify** – Resources and skills geared toward identification and management of the organization's risks, as well as overall cybersecurity program strategy. The typical areas covered under this function include asset management, architecture, governance approach, risk identification, and risk management strategy.
- **Protect** – Resources and skills geared towards developing and implementing safeguards to contain the effects of a potential cybersecurity event. Typical areas covered under this function include cybersecurity training, identity and access management, data protection and security, maintenance, patching, and protective technologies for technical, physical and administrative effectiveness.
- **Detect** – Resources and skills geared towards identifying the occurrence of cybersecurity events. The typical areas covered under this function include anomaly and event detection, security monitoring, and intrusion detection.
- **Respond** – Resources and skills geared towards responding to a detected cybersecurity threat. The typical areas covered under this function include response planning, communications, mitigation analysis, and continuous improvement of detection and response processes.
- **Recover** – Resources and skills geared towards responding to restore operations due to a cybersecurity incident or wide-scale disaster. The typical areas covered under this function include disaster recovery planning, communications, and overall improvements.

TLP:WHITE

Business and security interface – The three lines of defense

Too often, businesses think of security as a self-contained process: security is often “siloed” off by itself. But security is a comprehensive issue, and one that needs the involvement of the entire company. The success of the cybersecurity program is governed not only by the cybersecurity staff, but also by the close involvement and partnership with the business and audit functions. The cybersecurity program should be built with considerations for the interfaces and integration with other functions within the organization. One approach for defining the interface is provided within the “Three Lines of Defense” model, which provides a multi-layered approach and attempts to delineate the responsibilities for various groups.[3]

- **First Line of Defense (Operational Management)** – This group of employees own and manage the risk, while executing controls and associated procedures on a day-to-day basis. The operational management also enacts corrective procedures and takes appropriate actions in case deviation from the cybersecurity controls and procedures is identified.
- **Second Line of Defense (Risk Management and Compliance)** – The organization’s risk and compliance functions facilitate and monitor the implementation of the cybersecurity controls and procedures by the operational management. Cybersecurity risk is one of the broader risks being monitored by the second line of defense, and as such can correlate and report against other types of risks to the upper management. The second line of defense is considered a management function with limited independence on the operational management; however, it is not completely independent and needs additional oversight for proper monitoring of risk and controls.
- **Third Line of Defense (Audit Functions)** – Internal and external audit groups independently validate security controls and their effectiveness and provide their audit statements to board for their review and acceptance. This provides an independent check and balance mechanism to validate appropriate implementation of risk and control procedures and help monitor the current security posture of the organization and identify areas for improvement.

Headcount and expertise requirements

Organizations vary widely, and as discussed above, there is no "one size fits all" approach when determining cybersecurity spend, staffing, and headcount. Organizations should periodically analyze their staffing to confirm there is effective coverage within all cybersecurity departments. To try to ensure the right resource availability, the following are suggested minimum skill sets within the cybersecurity department:

- **Security Architecture** – Help define and maintain the enterprise security architecture in alignment with the organization's vision and security objectives. Further, these resources define detailed architecture for various solutions, technology, network, cloud, and other components of the environment.
- **Risk Management** – Focus on identification, assessment, and mitigation of cybersecurity risks by understanding the organization's business, technology, and security environment. They help organizations review inherent risks, identify associated technical, physical, and administrative controls, and further enact remediation plans to address risks in a methodical manner.
- **Identity and Access Management Specialist (IAM)** – Help manage employee, third party, and customer identities on the organization's infrastructure and applications. These resources also help govern access and authorization for users for information technology and systems.
- **Vulnerability Management and Penetration Testing** – Adept at identifying, classifying, and prioritizing security vulnerabilities across application, infrastructure, and other technologies, and help organizations reduce their exposure. Advanced skill sets include Internet of Things (IoT) security, mobile device vulnerability management, blockchain, and artificial intelligence. These professionals monitor networks and applications to determine existence of weaknesses and identify methods to remediate gaps.
- **Patch Management** – Maintain technology components and ensure appropriate vendor-developed patches and updates are deployed in a timely manner, in sync with identified vulnerabilities.
- **Security Monitoring Analyst** – Resources with broad-based skill sets who have the ability to monitor information system components using central consoles (e.g. event monitoring platform) and identify critical events of interest that could be potentially classified as security incidents.
- **Incident Response and Detection** – Tasked with responding to known detected threats and looking for ways to minimize the impact of an incident while allowing for smooth operations of underlying technology components and business processes. Once an anomaly is detected then it is triaged to determine next steps according to best practices.

Organizations should ensure they are providing adequate budgetary allowances to staff, train, and, retain skilled cybersecurity resources. There are several benchmarks in the industry to help guide organizations on budgeting and staffing. Overall, spending is on the rise—according to Gartner, in 2019 cybersecurity and IT risk budgets will increase by almost 9% year-over-year, reaching up to $124 billion.[4] 43% of the budget is attributed to employee growth within cybersecurity departments. International Data Corp. (IDC) estimates that organizations should spend between 7 and 10% of their IT budget on security.[5] According to the CISO Benchmark survey conducted by RH-ISAC in 2019, only 10% of companies said they spend more than 8% of their IT Budget on cyber security. The graph below shows survey results.

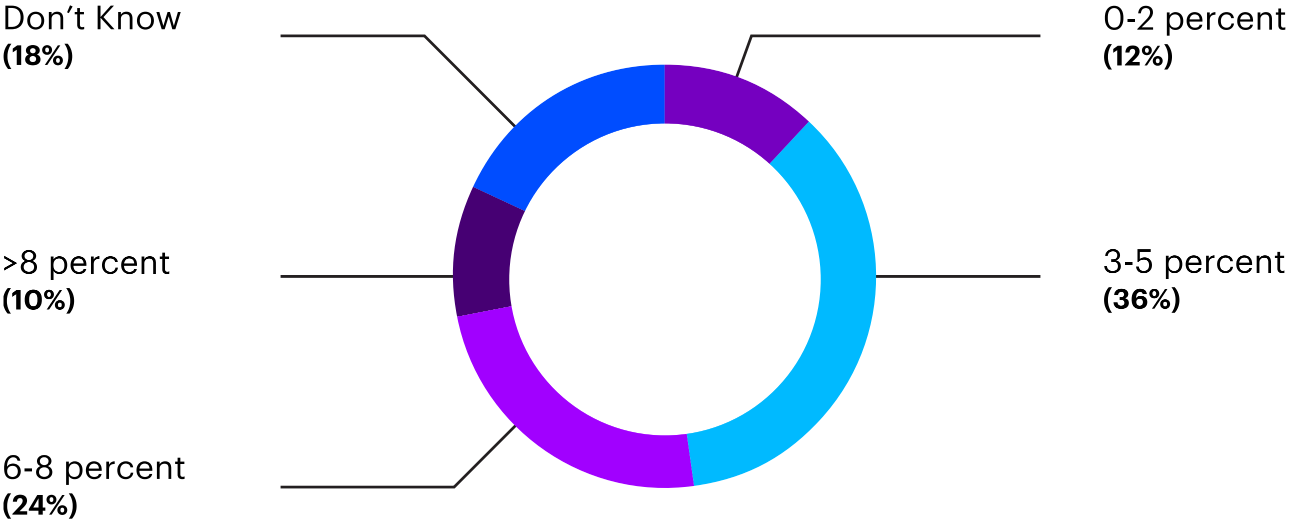
The Carnegie Mellon Software Engineering Institute examined various benchmark publications and other resources for CISOs that help determine the appropriate staff size and budgets for organizations.

Key data points include the following:[6]

- 3 to 6 information security staff per 100 IT staff
- 1.75 information security staff per 1 internal IT auditor
- 1 information security staff per 5,000 networked devices (workstations, switches, firewalls, servers, etc.)
- 3% to 11% of the total IT budget is allocated to information security

These statistics provide a reference point for staffing the cybersecurity function, but they aren't a one-size-fits-all. These results are highly dependent on company size and industry, and on the functions and activities that the CISO is responsible for performing and overseeing.

Percentage of IT budget dedicated to information security by RH-ISAC members, RH-ISAC annual CISO benchmark, 2019.



TLP:WHITE

Tools for evaluating existing cybersecurity staff

The National Initiative for Cybersecurity Education (NICE) framework released under the NIST Special Publication 800-181 is a great tool to consider when assessing an organization's existing cybersecurity department.[7] The use of the common vocabulary provided by the NICE framework enables employers to inventory and develop their cybersecurity workforce. The NICE framework can be used by employers and organizational leadership to:

- inventory and track their cybersecurity workforce to gain a greater understanding of the strengths and gaps in knowledge, skills, and abilities and tasks performed;
- identify training and qualification requirements to develop critical knowledge, skills, and abilities to perform cybersecurity tasks;
- improve position descriptions and job vacancy announcements selecting relevant knowledge, skills and abilities (KSAs) and tasks, once work roles and tasks are identified;
- identify the most relevant work roles and develop career paths to guide staff in gaining the requisite skills for those roles;
- establish a shared terminology between hiring managers and human resources (HR) staff for the recruiting, retention, and training of a highly specialized workforce.

Cybersecurity employment and attracting talent

According to the Bureau of Labor Statistics (BLS), employment for information security professionals is projected to grow 32% year over year from now until 2028 which is much faster than the average for all other occupations, which are expected to grow at 7% year over year.[8] The rapid growth is resulting in unavailability of skilled resources. As a result, to fill these critical roles organizations are finding creative ways to attract and retain cyber talent.

Here are a few strategies that can help attract cybersecurity professionals:

- **Internal training programs** – many organizations train internal employees to help retain and grow their departments with current employees. Creating an inventory of skill gaps can help determine which skill sets organizational leadership needs to retain and what skill sets they need to acquire.
- **Offering incentives** – this includes offering competitive salaries, benefits, paid time off, and support for professional and personal growth.
- **Joining local and national technology professional organizations** – cybersecurity professionals within the organization should consider joining boards at local and national cybersecurity groups to meet potential employees by networking.
- **Using the latest technology** – to help engage the younger generations, organizations should consider identifying and using career mobile apps that bring students and organizations together.
- **Encourage diversity** – Developing targeted programs to hire, train, and retain a diverse workforce can help to attract more people to the organization.

Additionally, based on a CISO Community Discussion hosted by RH-ISAC, some of the best practices from the retail and hospitality industry include the following:

- **Create an ambassador** – Look to increase awareness and generate internal interest by starting a "Security Ambassador Program" or similar program. This can help to help get the word out with other business leaders on specific challenges or issues, drum up talent, and build overall visibility.
- **Partner with educational providers** – several members mentioned participating as advisors to local college or university programs that offer cybersecurity training. These members report benefits on multiple fronts:
  - being able to tap into internship programs to build their talent pipeline
  - helping to shape cybersecurity program curriculum to include needed soft skills and other desirable components
  - raising awareness of their company's brand and image by helping to support the next generation of cybersecurity talent
- **Focus on soft skills** – one member shared how he focused his hiring strategy to include an enterprise security team of business information security leaders who could speak to non-technical leaders around the globe with a common language focused on cybersecurity risk and risk appetite.

PROCESS - PUTTING PEOPLE TO WORK

A big part of the success of an organization’s cybersecurity program relies on effective execution of key cybersecurity processes that help management achieve the program objectives in a consistent and reliable manner.

You can have the best people in place, using the most effective technologies, but if they don’t have a reliable process to follow, they can—and often will—still struggle.

Cybersecurity processes are designed to span across the enterprise and require support from several organizational functions for their successful implementation and execution. Process ownership starts from the top (e.g. CxO, Board of Directors, etc.) and works its way through the organization.

Well-designed cybersecurity processes are standardized, define clear accountability and ownership, align with the cybersecurity objectives, evolve over time, and allow for appropriate exception handling.

There is no finish line in cybersecurity, so it’s important to continue to develop and improve maturity levels around processes to maximize effectiveness of any cybersecurity program.

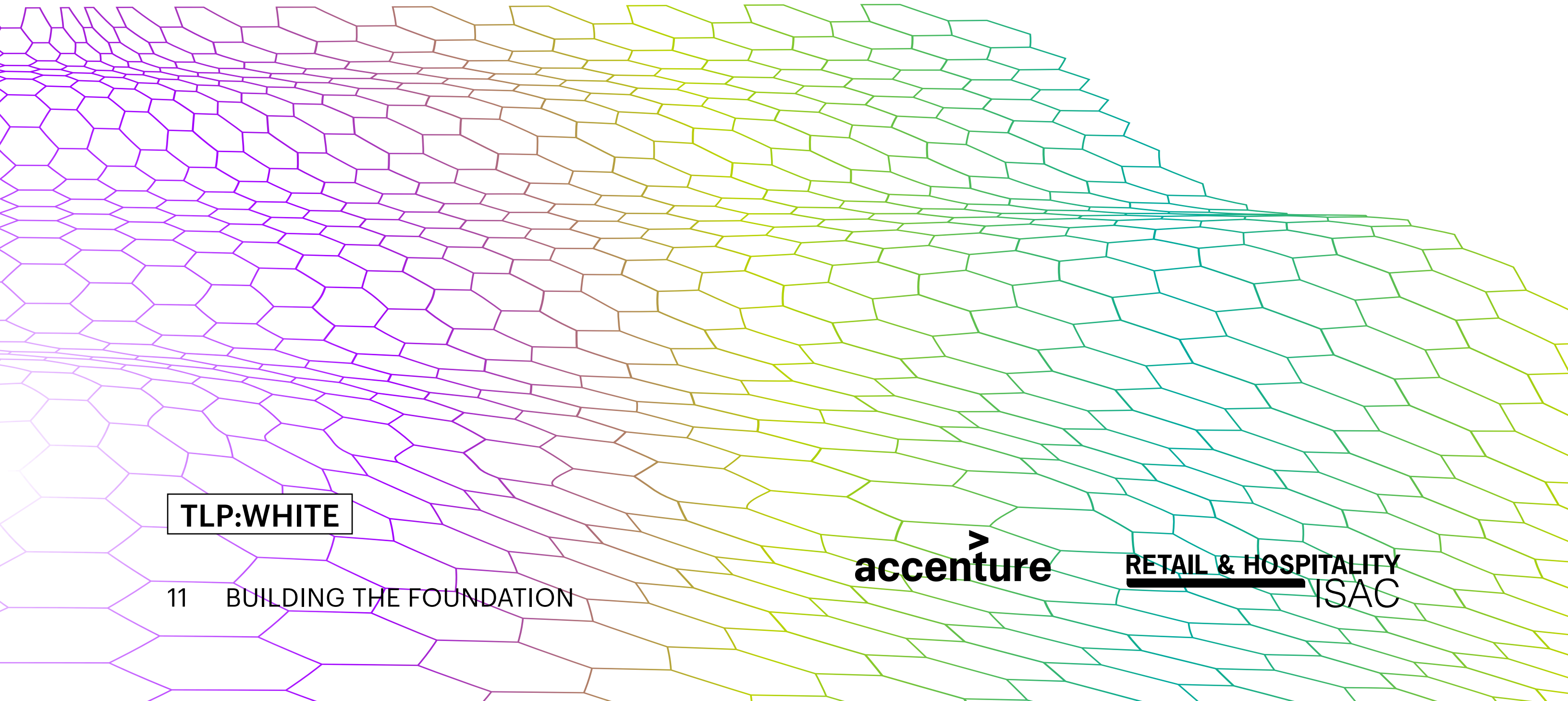
This sub-section provides insights into four key areas:

i. Key processes for an effective cybersecurity program

ii. Collaboration with other business functions

iii. Implementing continuous process improvements

iv. Nurturing a culture of security



Key processes for an effective cybersecurity program

There are thousands of cybersecurity processes established to govern day-to-day operations. Listed below are processes that a typical cybersecurity department covers to keep pace with potential threats and to help maintain a proactive security posture. These operational, management, and reporting processes are relevant for any size company:

- **Risk Management Process** (including privacy risk) – Identifying, monitoring, and managing potential risks to minimize threats. Privacy Impact Assessments help to determine data classifications and the potential privacy data and security risks of security projects.
- **Identity and Access Management** – Ensuring there are security controls and governing processes in place, so employees have appropriate access to information and files.
- **Security Monitoring** – Scanning all infrastructure and enterprise operations using logs and alarms to identify anomalies and help minimize risks.
- **Maintaining Technology and Security Appliances** – Verifying that all security tools used are inventoried, patched, have change management plans, and have a lifecycle roadmap to ensure their ongoing effectiveness.
- **Audit and Compliance Processes** – Monitoring employees and vendors to see if they are working within the policy that correlates with required mandates. Audit processes also assist in determining effectiveness of other processes and where improvements and enhancements may be necessary. Ongoing compliance changes around processing, storing, and transferring sensitive data requires organizations to monitor, track, and respond to changing compliance requirements.
- **Security Incident Response Process** – Preparing to respond to an incident. Every employee should be aware of their role in the event of an incident. An effective and well-communicated security incident response process helps organizations detect and respond to security incidents in a timely manner and potentially reduce the operational losses.

Implementing these processes helps cybersecurity teams to proactively try to prevent and respond to concerns in the event of a cybersecurity incident.

TLP:WHITE

Collaboration with other business functions

Cybersecurity processes extend and govern activities across the organization and can result in many interdependencies between cybersecurity and other business functions. It is vitally important that other functions provide support for cybersecurity initiatives and offer appropriate resources as necessary to make the cybersecurity initiatives a success. Identifying security "champions" across the organization can help communicate goals, foster relationships, and make security more "approachable" to individuals from other business functions.

Business functions that security often has interactions with include:

- **Individual Lines of Business** – It is critical for the core lines of businesses to integrate with the enterprise cybersecurity program and adhere to the policies established by the program for protecting the organization and customer data. For example, a business that needs to capture sensitive customer and financial data at point of sale terminals requires strong security controls and an understanding of business processes to develop a secure solution.
- **Privacy Office** – A privacy standard is set by the privacy office on how to process, protect, and manage sensitive data across its lifecycle. Privacy office and cybersecurity teams should work together to identify and classify sensitive data in order to put strong governance and security controls around it.
- **Legal Department** – The legal department assists with defining cybersecurity policies and procedures, specifically around legal implications of the policy manuals. They also play an integral part when reviewing third party contracts around risk and managing legal risk from security incidents.
- **Executive Management** (CIO/COO/CFO) – Security requires top-level management commitment to make the program successful. The executive management and organizational leadership need to know of the current security posture of the organization and should be informed periodically about the state of security by security leadership.
- **Procurement** – This department is instrumental when determining which security tools and services will be used. In many cases they also oversee the requirements for third parties that the organization works with to reduce any potential risk. There are several federal mandates required to do assessments to determine how third parties safeguard their networks.
- **Finance** – Many organizations have the finance department discuss potential projects to help determine the level of priority. Finance can assist with business impact analysis (BIA) to help determine the cost implications of a project.
- **Human Resources** – Human resources helps to identify, qualify and attract cybersecurity skills required for the organization.
- **Marketing** – The marketing department is concerned with protecting the brand and customer data in the retail and hospitality industry and is responsible for the roll out of digital customer experience initiatives which have additional cybersecurity implications.

TLP:WHITE

Implementing continuous process improvements

Cybersecurity is evolving continuously, and organizations should make every effort to establish continuous improvement processes to adapt their cybersecurity programs based on multiple drivers of change. The following outlines some of these key drivers along with guidance on how organizations can adapt:

External Drivers for Change

- **Growing Complex Threats** – As described in the Retail and Hospitality Threat Trend Report, Accenture iDefense and RH-ISAC analysis saw cybercriminals and cyber-espionage groups remain active throughout 2018. Retail and hospitality industries are increasingly targeted for the payments card data and the loyalty points data that they host, and payment card breaches continue to increase in frequency and volume.[9] Complex malware, advanced persistent threats (APT), ransomware, and other attacks are growing and ever-evolving. A threat-risk assessment conducted periodically will help the organization understand the changing threat landscape and update their program and processes to protect their assets.

- **Changing Regulatory and Industry Standards** – Over the past year, several security and privacy-focused regulations have been mandated by multiple geographical jurisdictions. Hospitality and retail organizations often span multiple geographies and need to keep up-to-date on the changing regulatory landscape specific to each region. A quarterly review of internal policies and security controls in alignment with regulatory requirements will help organizations to maintain adherence to regulatory requirements. External data sources providing analysis of updated regulatory requirements can be leveraged to review impacts to the risk and controls framework.

Internal Drivers for Change

- **Organizational Changes** – As the competitive landscape changes, organizations respond by updating their business models and revenue streams. This leads to changes in strategy, operations, and other organizational re-structuring (including people movement). Organizations should review their cybersecurity risks before, during, and after any major restructuring, and update the cybersecurity program as part of their change management function. Any major people movement should automatically trigger review of key cybersecurity processes.

- **Data Consumption and Associated Technology Evolution** – With the advent of new technologies in the retail and hospitality sectors (e.g. IoT in supply chain, digital apps for room check-in, etc.), organizations are changing the way they are using customer data and how external access is granted to sensitive information. With changing data consumption and underlying delivery technology, changes are warranted in the security architecture, privacy and security policies, security assessment frameworks, and core technology implementation for data protection (e.g. cloud-based data loss prevention to prevent data exfiltration stored on cloud platforms through a vulnerable application).

Inherent Process Issues

- **Inherent issues within certain cybersecurity processes** are typically identified by participating actors once the processes are released for consumption. For example, incident response processes are often updated by following table top exercises (for simulation) as well as after security incidents or major security breaches. Cybersecurity processes should have mechanisms to update them as part of their ongoing operations.

TLP:WHITE

Nurturing a culture of security

As we've stressed throughout this guide, cybersecurity should be, ultimately, everyone's responsibility within the organization. A good way to help create and sustain a culture of cybersecurity is to deploy more usable and practical cybersecurity processes, which reduce friction and are easier to follow by various business functions. Making sure that there is clear and consistent communication on cybersecurity policies and processes within the organization helps keep team members apprised of developments and increases their adherence to the processes.

Below are a few methods to help be effective at disseminating the organization's cybersecurity message:

- Provide regulatory and policy updates at quarterly or bi-annual cybersecurity meetings
- Have ongoing cybersecurity training via web and face-to-face to make it interactive
- Share cybersecurity news and updates via corporate communication channels, such as through company newsletters or emails
- Create a cybersecurity awareness month
- Partner with national and state cybersecurity initiatives
- Promote good cybersecurity hygiene with contests

TECHNOLOGY – THE TOOLS OF THE TRADE

In this section, we review the technologies required to operate an effective cybersecurity program. Specifically, we discuss common technology frameworks, how to prioritize technology implementation, maximizing existing spend, and partnering with other departments to maximize your budget.

Technology plays a crucial role in effective implementation of an organization's cybersecurity program. A multitude of tools and technologies exist in the market that organizations need to carefully review and deploy to achieve their program objectives.

Organizations should develop an enterprise security architecture and select appropriate technologies based on their ability to meet the defined objectives. The aim should be to maximize the return on technology investments while meeting the needs of the cybersecurity program and minimizing overlap in capabilities. This sub-section provides a primer on the following areas:

i. Selecting the appropriate technologies with minimal costs

ii. Prioritizing technology implementation

iii. Partnering with other functions for technology spend

Selecting the appropriate technologies with minimal costs

The cybersecurity market is flooded with tools and technologies, making it increasingly difficult to select the right solutions to meet the organization's security objectives, particularly if you're working with limited budgets and experienced staff. Organizations should build a technology selection framework that aligns with the enterprise technology and security architecture.

These steps can provide a high-level approach for making procurement decisions, as well as for ongoing rationalization of tools and technology:

Step 1 – Assess Cybersecurity Risks

Conduct an enterprise-wide cybersecurity risk assessment to identify key risks and associated risk mitigation strategy.

Step 2 – Spend Analysis Driven by Risk

Review the organization's security budget and allocate spend in proportion to the risks identified previously.

Step 3 – Capability Mapping

Identify key cybersecurity capabilities and associated controls that would help mitigate the identified risks. Prioritize capabilities based on security vision and goals, and alignment with business objectives.

Step 4 – Tools Analysis and Rationalization

For prioritized capabilities, identify potential tools and technologies that the organization may possess or needs to acquire. Rationalize tools in a progressive manner by deploying foundational tools first that provide broader coverage and then moving toward advanced tools that target specific areas.

Step 5 – Periodic Assessment of Implemented Tools

A periodic review of technology implemented by the organization would help identify ones which are redundant, barely used, or require additional capacity to maintain performance. These assessments would also help identify capabilities that are no longer necessary or ones that have not been adequately catered to with existing tools.

Prioritizing technology implementation

Technology implementation projects can sometimes be initiated in a siloed manner, creating a disconnect with the organization's strategy and the impact of a cybersecurity project. The siloed approach can create serious inefficiencies, as similar projects with overlapping capabilities may be executed in distinct groups across the organization. This can put additional stress on resources around people and technologies. Organizations should consider a macro-level approach when determining which projects to move forward with and should consolidate projects that overlap with other departments to reduce costs and improve organizational alignment.

The following are recommendations for prioritizing technology implementation projects:

- **Host organizational strategic-level cybersecurity planning meetings** – Meet with the leadership team to understand which projects are deemed high priority across the organization. Following that, assess and determine what projects are high priority and which ones can be consolidated across departments. This will require periodic strategic planning sessions and will help the organization to focus on high priority projects. It is also ideal to set metrics and milestones to keep track of progress.

- **Identify priority factors** – As part of project selection process, ask the associated stakeholders to identify and explain the purpose of a project, what impact the project will have, what the potential loss of not executing the project would be, and other reasons for project consideration and approval.

  Some areas to review for potential cybersecurity projects include:

  – Risk mitigation

  – Customer enhancement

  – Industry advantage

  – Cost reduction

  – Federal, state or local mandate requirement

  – Improved quality

  – Profit opportunity

  – Business operations improvement

- **Return on Investment (ROI) analysis** – Review the overall financial implications of individual cybersecurity projects against the perceived benefits to determine the ROI. Prioritize projects with higher ROI or earlier break-even of the costs, as they would result in the maximum effectiveness of employed capital.

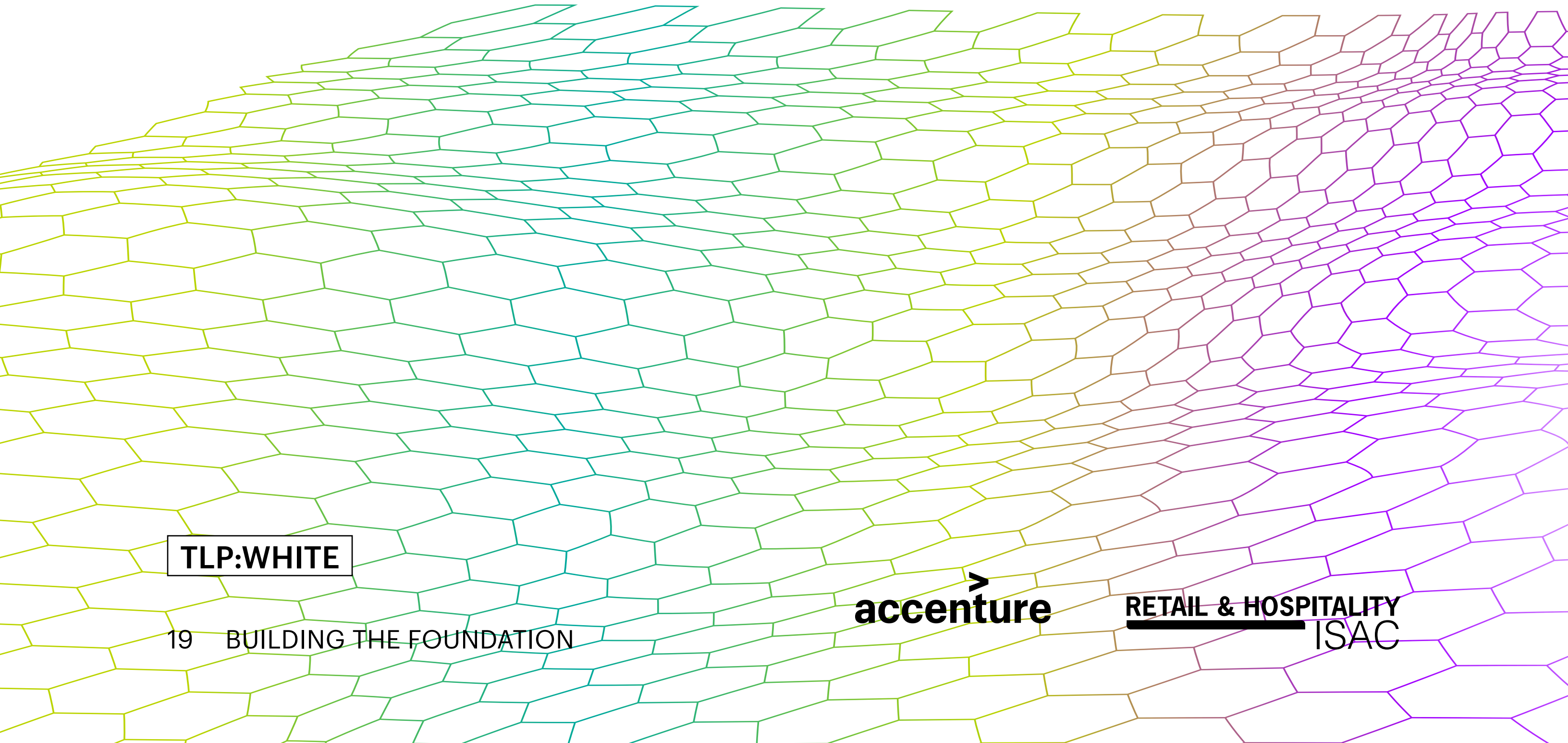
- **Resource validation** – Significant resource commitments may be required to execute critical cybersecurity projects. This may result in unavailability of resources to perform existing functions or responsibilities, thereby reducing overall effectiveness of the cybersecurity program. Resource validation should include an analysis of resources needed to implement the project, provide ongoing support after stabilization, and to continue performing existing capabilities without any reduction in performance.

Partnering with other functions for technology spend

One useful strategy for the security group to maximize available funds is to partner with other organizational functions in deploying technology solutions that meet both business and cybersecurity needs. Many functions, specifically the internal ones, require technology to perform their day-to-day operations which also have capabilities that could be utilized by the security group (e.g. ERP systems for finance function, service management and ticketing platforms for IT function, etc.). By partnering with such functions, security teams can ensure that the right tools are selected by the business from the start and that security capabilities are considered when performing the tool selection.

The following are some recommendations on partnering for technology spend:

- Identify business functions with potential overlaps in technology capabilities
- Validate synergies for partnership with other functions
- Require the program management office to monitor projects across the organization and help identify which projects can be combined for technology spend
- Interface with the procurement team to consider combining budgets for similar technologies and projects initiated by other functions
- Maintain a list of security capabilities that needs associated technologies, and identify which ones could have a value proposition for other functions—thereby allowing for proactive collaboration with the other functions



OVERSIGHT – WATCHING THE WATCHMEN

An oversight function is critical to help determine potential risks and to identify areas to improve the cybersecurity program.

Clearly established accountability and responsibilities help organizations maintain the direction and effectiveness of the cybersecurity program, helping to achieve the team's goals and objectives. Below are some of the key oversight functions for a typical cybersecurity program:

Board of Directors and Executive Management

Board members and executive management should understand cybersecurity to ensure the proper questions are being asked from the cybersecurity team. It is recommended to have regular meetings between the security leadership and the board to help identify potential risks and discuss remediation plans. In case of neglected responsibilities, the board could be held responsible in litigation, and insurance claims could potentially be denied due to non-compliance of the policy requirements when safeguarding systems. Audit committees can be set up to further enable and apprise the Board of Directors, and are instrumental to improving visibility on cyber security issues.

According to Accenture Security, cybersecurity briefings to the board should capture the following key components:

- Threats to the organization's most important lines of business and how those threats are changing
- Activities the business is doing to protect itself from cyber-attacks and their effectiveness
- Strategic options and initiatives in-flight across the business, and what the security leadership is doing to manage the inherent risks
- Residual risks and what the business needs to do about them

Understanding these items can position the board to be in a better place to help shape cybersecurity challenges and issues.

Operational Management

Operational management assists with the crucial monitoring of day-to-day activities supporting the cybersecurity program. They align with the executive management's vision and ensure adherence to the processes established as part of the program, providing tactical oversight on staff. The operational management should be kept current of any changes to the program vision and goals and empowered with appropriate administrative and technical solutions to execute their responsibilities.

TLP:WHITE

Audit

Internal and external audits (third line of defense) are important to validate technical, physical, and administrative controls effectiveness. Independent audits help identify gaps and create remediation plans to help mitigate risks. Internal audits help organizations police themselves where external audits include an outside third-party to help identify high risk controls. At the minimum, annual audits should be conducted for the cybersecurity program and an audit issues remediation plan should be developed and socialized with the board.

Metrics and Reporting Dashboards

Ongoing monitoring and reporting of key metrics for the cybersecurity program helps ensure that the program stays on-track with its objectives and instills confidence in its effectiveness. Metrics also enable leadership to take corrective action in case the program is deviating from its objectives.

Organizations should carefully select appropriate Key Performance Indexes (KPIs) and Key Risk Indicators (KRIs) to be reported to the management. Interactive dashboards help in communicating the metrics in the most effective manner, however reports should be tailored to the audience (e.g. executive management reports, operational management reports, etc.).

External Regulatory Oversight

Regulatory frameworks and other industry standards are requiring organizations to deploy additional controls and provide appropriate oversight on their cybersecurity program. Adherence to appropriate regulations and standards provides organizations with the right guidance and direction to meet the cybersecurity requirements.

Action Items

As you begin to think about the organization of your security program, think about the organization of your company as a whole, and how security can fit in.

How big is my IT infrastructure, and how many people might I need to manage security?

Do I have people in place already with security expertise? If not, do I have a strategy for attracting more?

How do the departments within my organization work together? Where are the pain points? How does security fit into the bigger picture?

What policies and processes are already in place around security? How have they been implemented?

What technology do we currently have in place? Is it well-inventoried and documented?

What is our need for expanding that technology, and do we have the budget for it?

What kind of governance and oversight do we have in place overall, and with regard to security specifically?

What kind of reporting and measuring do we currently do on our security practices?

TLP:WHITE

References

[1] "Gartner Top 7 Security Risk Trends for 2019", Smarter with Gartner, June 19, 2019. https://www.gartner.com/en/human-resources/research/talentneuron/cybersecurity-labor-shortage-and-covid-19.

[2] "Framework for Improving Critical Infrastructure Cybersecurity", National Institute of Standards and Technology, April 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[3] "Three Lines of Defense", The Institute of Internal Auditors, June 2019. https://na.theiia.org/about-ia/PublicDocuments/3LOD-IIA-Exposure-Document.pdf.

[4] "Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019", Gartner Newsroom, August 15, 2018. https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019.

[5] "How much should you spend on security?", CSO, August 20, 2019. https://www.csoonline.com/article/3432138/how-much-should-you-spend-on-security.html?upd=1566483968575.

[6] "Structuring the Chief Information Security Officer Organization", Carnegie Mellon University, September 2015. https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf.

[7] "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework", National Institute of Standards and Technology, August 2017. https://csrc.nist.gov/publications/detail/sp/800-181/final.

[8] "Occupational Outlook Handbook" Bureau of Labor Statistics, September 4, 2019. https://www.bls.gov/ooh/computer-and-information-technology/information-securi,ty-analysts.htm.

[9] "Retail and Hospitality Threat Trend Report", Accenture, Retail & Hospitality ISAC, 2019. https://www.accenture.com/us-en/insights/consulting/retail-hospitality-threat-trend-report.

[10] The Cyber-Committed CEO and Board" Accenture Security, 2017. https://www.accenture.com/_acnmedia/pdf-42/accenture-cyber-committed-ceo-and-board-pov.pdf.

Contacts/Authors

Accenture

CJ Cui
Managing Director
North America Retail Security
cj.cui@accenture.com

Nikhil Kaduskar
Manager, Security Strategy and Risk
nikhil.kaduskar@accenture.com

Derek Miller
Consultant, Security Strategy and Risk
derek.miller@accenture.com

RH-ISAC

Amy Tate
Program Director, Intelligence
amy.tate@rhisac.org

About Accenture

Accenture is a leading global professional services company, providing a broad range of services in strategy and consulting, interactive, technology and operations, with digital capabilities across all of these services. We combine unmatched experience and specialized capabilities across more than 40 industries—powered by the world's largest network of Advanced Technology and Intelligent Operations centers. With 509,000 people serving clients in more than 120 countries, Accenture brings continuous innovation to help clients improve their performance and create lasting value across their enterprises. Visit us at **www.accenture.com**.

Disclaimer: This document is intended for general informational purposes only and does not take into account the reader's specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this presentation and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.

About the RH-ISAC

The Retail & Hospitality Information Sharing and Analysis Center (RH-ISAC) is the trusted community for sharing sector-specific cyber security information and intelligence. The RH-ISAC connects information security teams at the strategic, operational and tactical levels to work together on issues and challenges, to share practices and insights, and to benchmark among each other – all with the goal of building better security for the retail and hospitality industries through collaboration.
RH-ISAC serves all retail and hospitality companies, including retailers, restaurants, hotels, gaming casinos, food retailers, consumer products and other consumer-facing companies.
For more information, visit **www.rhisac.org**.

200432