Cybersecurity is Everyone's Job

A Publication of the National Initiative for Cybersecurity Education Working Group
Sub-Group on Workforce Management
at the National Institute of Standards and Technology

Draft: For Public Comment

Introduction

The human is the greatest vulnerability in any organization.

In this era of persistent cyber threats, an organization will be secure only with the active participation of everyone. Unfortunately, many organizations limit security responsibilities to designated security personnel that perform specialized security functions. But effective security must be enterprise-wide, involving everyone in fulfilling security responsibilities. Each member of the group, from the newest employee to the chief executive, holds the power to harm or to help, to weaken or strengthen, the organization's security posture.

This guidebook outlines what each of us should do to protect the organization, based on the types of work we do.

Benefits of this Guidebook

- Helps you to know what you need to do, based on your role
- Engages all functions and roles—technical and non-technical—in securing critical information and systems
- Provides essential, must-do-first guidance in plain language
- Turns the organization's greatest vulnerability—its people—into the organization's greatest asset

Why this Guidebook is Needed

From critical information systems holding sensitive data (Information Technology, or IT), to critical operational systems running physical processes (Operational Technology, or OT), every organization today depends on their technology to be successful. Even those entities that do not maintain a robust technology environment must still operate in a world that depends on IT and OT—and the humans that own, manage, and use those systems.

Contrary to the common misunderstanding that cyber threats are a technology problem looking for a technology solution, the data clearly and consistently shows that employees are the greatest vulnerability of any organization. This means that no matter how robust the technology is, or how many cybersecurity policies the Chief Information Security Officer (CISO) may have introduced, the organization cannot be secure without all individuals doing their part, across all business functions, technical and non-technical.

Consider how dependent our public health is on the active participation of everyone. We are all educated and encouraged to exercise good hygiene such as washing hands and seeking preventative care through immunizations, and even children are well versed in best practices for covering your mouth when you sneeze, handwashing and so forth. However, even when well-trained medical professionals are delivering exceptional care in a robust health care system, the spread of diseases is primarily prevented through good hygiene. Similarly for good "cyber hygiene," when each of us takes appropriate care, we protect the larger community.

Another common misunderstanding is that organizations just need to hire more technically-savvy cybersecurity professionals. Without a doubt, these skilled people are very important. Without them, essential technical safeguards could not be implemented, ongoing security operations would not be conducted, and there would be no one to respond to the next cyber incident. However, the largest "attack surface" of the organization is you and me—the people who perform common functions: Leadership, Planning, and Governance; Sales, Marketing, and Communications; Facilities, Physical Systems, and Operations; Finance and Administration; Human Resources; Legal and Compliance; and routine Information Technology operations. Therefore, cybersecurity is everyone's job.

Who Can Use this Guidebook?

This guidebook is intended for every kind of organization, from large government agencies and publicly-traded corporations to nonprofits and small, family-owned businesses, since all organizations must perform common, essential activities. These functions include generating revenue, communicating with external customers and stakeholders, delivering products and services, leading people, and managing financial and legal matters. Each of these areas routinely exposes the organization to a variety of cyber-related business risks. To reduce these risks, each person in each business function must be involved, understanding your role and taking individual responsibility for mitigating cyber risks.

In the following pages, you'll find practical guidelines for action, organized by business function. Many of these tasks are simple… so simple that they might seem inconsequential. But these guidelines reflect proven best practices developed by security experts from government, industry and academia.

The cybersecurity of your organization depends on you, and here's what you can do.

How to Use this Guidebook

This guidebook is organized by business function—those essential activities which all organizations must perform to at least some extent. Each function represents work that may be performed by a number of formal job roles, or they may be performed by one person, depending on the size of the organization. They are intended for full-time employees, part-time hires, leaders at all levels, and those who perform tasks in that particular business function, even if their primary role is elsewhere. The goal is to build a cyber-secure workforce, with each person doing their part to secure the organization. The business functions are presented as seven categories:

- » Leadership, Planning, and Governance
- » Sales, Marketing, and Communications
- » Facilities, Physical Systems, and Operations
- » Finance and Administration
- » Human Resources
- » Legal and Compliance
- » Information Technology

Each section is written so that it may be used as a standalone reference for that particular business function; therefore, some of the guidelines will appear in multiple sections.

Additional resources, references and information on how this guidebook was developed are contained in the appendices.

Please note that the information in this guidebook is not intended to replace your organization's security policies; rather, it provides a supplemental quick reference of actions that each person can perform to ensure the organization's cyber resilience.

This document can be shared as-is, or organizations may tailor it to their needs and communication methods—in materials such as booklets, webpages, publications, or webinars. The intent is for users to understand how everyone in an organization—across all business functions and roles—can enforce the cybersecurity posture of their organization.

Building a Cyber-Secure Culture

First, a word on culture. Your organization's culture is critical to establishing a successful cybersecurity posture. Without a culture that emphasizes, reinforces, and ultimately drives behavior toward security, the necessary conditions will not be set. In other words, a resilient workforce will not exist without a cyber-secure culture.

Mindset

Mindset is a critical component of culture. When we build awareness into the organizational culture, we increase our readiness to address cyber risks and we help keep our collective eyes open. Whether you work in a small non-profit or a Fortune 100 company, every organization is at risk. Given the prevalence of cyber attacks, we need to stay prepared. Collectively, the appropriate behaviors at the individual level will contribute toward the resilient workforce that every organization needs. And behaviors are driven by mindset.

Leadership

Your organization's leaders set the tone. No factor is more significant to impacting awareness and mindset than leadership. Leadership, by example and emphasis, becomes the basis of a cyber-secure culture. In practice, this means the personal example of individual leaders, as well as their emphasis to team members, to embrace cybersecurity education, awareness and best practices. It is important for leaders to understand that deep technical knowledge is not required; rather, an open and honest approach to improving personal security habits based on sound guidelines, shared with others, is what matters. Simply put, leadership involvement is the single most important factor for a cyber-secure organization.

Training and awareness

Once leaders are involved in fostering and participating in a cyber-secure culture, the next step is to implement employee awareness training. This will help to build a more complete understanding of risks, and—most importantly—provide specific steps for mitigating them. Training programs come in many forms, but most involve a series of computer-based learning modules and practical exercises. Formal training is designed to increase awareness of various attack forms and methods, and how to react to them, as well as the company's required security practices. One area of increasing concern is the use of social engineering, or manipulation, to spread exploits via unsuspecting employees. They may have access to the targeted data or system; or may be used to continue spreading malware to others who do. As a result, hardening your employees to the reality of socially engineered concerns is a key element in a training program. No program will lead to a sustained 100% success rate against human factor-based exploits, but they can substantially reduce the volume, and potentially even the impact, of attacks. By reducing volume, your cyber defenders can focus on a smaller, more manageable set of incidents.

Another common way to help build cyber-secure culture is through internal awareness campaigns; there are numerous creative ways to get the message across. From posters and newsletters to contests and prize drawings, organizations have found effective ways to generate "buzz" around important themes. While these methods should be employed year round, National Cybersecurity Awareness Month, observed in October, is a particularly good time to emphasize these themes.

Performance management

As change management professionals will attest, a proper set of incentives and disincentives can have a profound impact on human behavior. For real cultural change to occur in cybersecurity preparedness, individual performance goals must align with the goals of the organization. In most cases, individual goals are already comprised of a combination of quantifiable metrics and qualitative targets. Performance goals in security can include completion of required training, improved responses to phishing exercises, compliance with policies, and avoidance of risky online behaviors. Financial and operational metrics are common in organizations; security-related metrics should be also.

Technical and policy reinforcement

Finally, specific technical controls associated with human behavior can be implemented to reinforce cyber-secure culture. While controls are generally implemented to mitigate the risks of failures in human behavior, they also have the effect of reinforcing culture, since they tend to funnel behaviors down acceptable paths. Just as physical access controls reinforce the mental awareness of a physical perimeter, so can password policies, multi-factor authentication and mobile device management solutions reinforce security culture, albeit in a modest and indirect manner, by reminding users of the need for cybersecurity. Policy at the organizational level can also motivate and influence implementation of controls by outlining the consequences of non-compliance.

There are many ways that these guidelines can be implemented, reflecting the unique values, personalities and activities of each organization. What matters is that they form the basis for developing a cyber-secure culture by increasing awareness and fostering the right mindset. With a sound cyber-secure culture in place, each business function can focus on its own unique contribution towards protecting the organization.

Leadership, Planning, and Governance

Setting overall direction, establishing priorities, maintaining influence, and mitigating risks

What Leadership, Planning, and Governance does

If you are responsible for the overall strategic direction of the organization, or for maintaining controls and mitigating risks, this section applies to you. Leadership, Planning, and Governance professionals are often the most senior leaders, or are directly supporting strategic decision makers. You may be involved in board proceedings, contribute as senior level management or manage a complex government agency, with fiduciary responsibility and budget authority. Or, you could be the owner-operator of a small business or franchise. What all these roles have in common is that final decisions are made by you, or you are supporting those who make those decisions. Because competing demands must be balanced and limited resources allocated, you play a crucial role in establishing priorities and ensuring adherence to them. At the same time, strategic risks to the organization must be addressed. You are often the arbiter of difficult decisions.

You matter to the organization, because without you, the organization lacks direction and cohesion. You are the hub of the wheel—connecting to, coordinating, and driving the many parts of the business.

The role of Leadership, Planning, and Governance in cybersecurity is all about:

- Managing and mitigating overall cyber-related business risks
- Establishing effective governance controls
- Prioritizing and resourcing cybersecurity programs
- Safeguarding the sensitive information you rely on for planning and decision making
- Establishing a cyber-secure culture within the organization

What Leadership, Planning, and Governance professionals should do:

- Understand cybersecurity well enough to enable sound decision making
  - » Establish a routine reporting process for cyber risks within the organization
  - » Engage with trusted third parties to learn about cyber risks and their mitigations—this includes consultants, industry groups, and cybersecurity service providers and educators
  - » Regularly commission objective risk assessments of the organization
  - » Implement cybersecurity best practice frameworks, maintained by authoritative entities such as the National Institute of Standards and Technology (NIST), Center for Internet Security (CIS), and International Organization for Standardization (ISO)
- Include cyber risks in the enterprise risk management process
  - » Avoid treating cyber risks as a separate and mysterious matter only for technologists
  - » Understand the organizational impacts of cyber incidents
  - » Consider risks introduced by partners and suppliers
  - » Conduct exercises and decision-making drills to familiarize yourself and your organization with how to respond
  - » Prioritize cyber-related risks to ensure appropriate attention and effort is committed to their mitigation
- Develop and maintain organizational information security policies and standards
  - » Ensure that information security policies are informed by risk assessment, regulations, and standards / best practices
  - » Ensure organizational security policies are appropriately implemented, institutionalized and communicated
  - » Be aware of relevant data protection / privacy regulations and legislation to ensure that your organization remains in compliance, e.g., General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Manage-

Your title includes words like…

Director, Board, Chairman, Chief, President, Partner, Principal, Owner, Founder, Secretary, Consultant, Strategy, Governance, Risk, Intelligence, Controls

Information and systems you own, manage, or use

- Strategic plans
- Board and senior management proceedings
- Financial records
- Merger and acquisition information
- Third-party recommendations and reports
- Routine communications of a sensitive nature

ment Act (FISMA), Freedom of Information Act (FOIA), Sarbanes-Oxley (SOX), Family Educational Rights and Privacy Act (FERPA)
    - » Have a schedule in place to regularly review and update policies
- Promote the development of effective cross-functional teams to accomplish cybersecurity goals for the organization.
- Adequately fund cybersecurity resource requests
    - » Digital assets cannot be protected without human and technical resources; be ready to commit resources aligned to a cohesive cybersecurity strategy
    - » Plan for future needs
- Protect sensitive strategic, financial, legal, and risk information
    - » Share only necessary information
    - » Ensure the information is retained/destroyed in compliance with the organization's data retention policies or external regulations
    - » Use encryption, passwords, and other methods to secure files when you transfer them to others
- Protect access to online file sharing or decision support platforms by applying best practices, such as:
    - » Strong, complex passphrases
    - » Unique passphrases for each critical account
    - » Multi-factor authentication

What we all should do:

- Use social media wisely
    - » Apply strong privacy settings
    - » Don't share personal information on business accounts
    - » Don't share business information on personal accounts
- When working from home, secure your home network by applying best practices (see NIST SP 800-46 Rev. 2), such as:
    - » Change your wireless router password, SSID, and limit ability of others to find it
    - » Maximize encryption levels on your wireless router
    - » Increase privacy settings on your browser
    - » Use Virtual Private Networks (VPN) to access corporate networks whenever possible
    - » For additional security, protect browsing privacy through encrypted browsers
    - » For additional security, protect personal email accounts through encrypted email
- When traveling, secure your connections to the enterprise:
    - » Do not enter sensitive information on public computers
    - » Use VPN access to corporate networks whenever possible
    - » Do not use public Wi-Fi without VPN
    - » Use a dedicated wireless hotspot for internet access
    - » If a hotspot is not available, consider tethering to a corporate or business-issued cell phone
    - » Physically protect your computer from theft and unauthorized access

A note to leaders:

You are ultimately responsible. The organization will not be cyber-secure until you are actively involved in understanding, prioritizing, speaking about, and leading by example in protecting digital assets. Work with cybersecurity experts—externally and those you hire internally—to establish sound guidelines, be familiar with those guidelines, implement them yourself, and ensure that your teams know what they're expected to do.

Don't be afraid to ask questions. Nobody expects you to understand cyber as well as you understand finance or operations, but everyone expects you to mitigate risks to the business—and cyber risks are real. Your job depends on how well you address the real risks of an often-unfamiliar subject.

Sales, Marketing, and Communications

Raising awareness, communicating, generating revenue, and interacting with customers

What Sales, Marketing, and Communications does

If you are interacting with customers, clients, donors or citizens, this applies to you. Sales, Marketing, and Communications professionals are those who engage prospective and existing customers to drive awareness of products and services, stimulate interest, and generate revenue through sales or other means. You may also be involved in public- and media-facing communications. You are the messengers of the organization, carrying news of the good things you provide to those who need to know, and responding to current events. This includes the crucial work of converting business ideas into real business deals. Along with the people who deliver the products or services, you are often the most visible, outward-facing people in your organization.

You matter to the organization, because without you, ideas, products and services sit idle—you make the organization a vibrant part of the world around it.

Your title includes words like…

Sales, Accounts, Client, Revenue, Donor Relations, Advertising, Social Media, Marketing, Demand Generation, Communications, Media Relations, Analyst Relations, Public Affairs, Community, Stakeholder, Engagement

Information and systems you own, manage, or use

- Customer data
- Partner data
- Contracts
- Financial data
- Customer Relationship Management (CRM) systems
- Customer support portals
- Press releases
- Public announcements
- Public-facing websites
- Social media accounts

The role of Sales, Marketing, and Communications in cybersecurity is all about:

1. Establishing and protecting the company brand, reputation and the trust of citizens, customers, and partners
2. Preventing/limiting information loss as you interact with the outside world
3. Reducing risks to the enterprise network presented by remote work, telecommuting, and travel

What Sales, Marketing, and Communications professionals should do:

- Communicate the importance of cybersecurity matters to your stakeholders
  - » Access reputable sources to develop a well-rounded understanding of how information and systems fit into the ecosystem of the people you interact with—this includes consultants, industry groups, cybersecurity service providers and educators
  - » Understand the potential impact to your organization of a cyber incident
  - » Inventory the types of information entrusted to the care of your organization, and consider the potential impact of data compromise for your customers and partners
- Develop a communications plan for the inevitable cyber incident
  - » Participate in internal incident response team planning
  - » Become familiar with the cyber incident response plan
  - » Participate in "table-top exercises" and other planning efforts in anticipation of cyber incidents
  - » Draft a communication plan consistent with regulatory requirements, legal considerations, industry best practices, and commitments made to external stakeholders
- Protect shared files
  - » Use encryption, passwords, and other methods to secure files when you transfer them to/from customers and partners
- Protect access to your Customer Relationship Management (CRM) platform by applying best practices, such as:
  - » Strong, complex passphrases
  - » Unique passphrases for each critical account
  - » Multi-factor authentication
  - » Restricting levels of access by need

  - » Removing employees or vendors when they are no longer involved
- Protect customer information in quotes, purchase orders, invoices, payments, and presentations
  - » Share only necessary information
  - » Ensure the information is destroyed in compliance with the organization's data retention policies or applicable regulations
- Be aware of the implications of conducting business in foreign jurisdictions with different regulations such as the European Union's General Data Protection Regulation (GDPR)

What we all should do:

- Use social media wisely
  - » Apply strong privacy settings
  - » Don't share personal information on business accounts
  - » Don't share business information on personal accounts
- When working from home, secure your home network by applying best practices (see NIST SP 800-46 Rev. 2), such as:
  - » Change your wireless router password, SSID, and limit ability of others to find it
  - » Maximize encryption levels on your wireless router
  - » Increase privacy settings on your browser
  - » Use Virtual Private Networks (VPN) to access corporate networks whenever possible
  - » For additional security, protect browsing privacy through encrypted browsers
  - » For additional security, protect personal email accounts through encrypted email
- When traveling, secure your connections back to the enterprise
  - » Use VPN access to corporate networks whenever possible
  - » Do not enter sensitive information on public computers
  - » Do not use public Wi-Fi without VPN
  - » Use a dedicated wireless hotspot for internet access
  - » If a hotspot is not available, consider tethering to an issued cell phone
  - » Physically protect your computer from theft and unauthorized access

A note to leaders:

Implementing cybersecurity best practices is hard to do with external-facing employees, particularly if they are out in the field most of the time. The most effective aspect of leadership is to lead by example: know these guidelines, implement them yourself, and ensure that your teams understand what they're expected to do.

Demand cyber-secure resources. If your organization does not provide secure connections, such as multi-factor authentication, VPN, and/or mobile hotspots, *demand it*! Your job, and the organization's reputation, depends on maintaining the trust of citizens, customers, and partners.

Facilities, Physical Systems, and Operations

Designing and delivering products and services, managing operations, and maintaining the physical environment

What Facilities, Physical Systems, and Operations does

If you are designing and delivering the organization's core products and services to your customers, or are part of the core operations to support delivery, or are managing and maintaining the physical environment, this section applies to you. Since the types of products and services vary greatly, Facilities, Physical Systems, and Operations covers a diverse range of roles from site management to product engineer to operations analyst to distribution manager, and beyond. You deliver the organization's value to the world, fulfilling its primary purpose. Your role directly impacts citizens, customers, and partners who depend on your organization's products and services.

You matter to the organization, because successful development and delivery of its products and services depends on you. The organization would cease to function without the capabilities you provide, and the primary purpose of the organization would go unfulfilled. Your performance is also crucial to maintaining a competitive advantage—what makes your organization unique and respected—in a crowded, noisy, and busy world. Furthermore, the technology systems you operate, including those that enable physical processes (Operational Technology (OT), rather than Information Technology (IT)), come with potential risks to life and limb, making your security readiness paramount.

Your title includes words like…

Operations, Delivery, Consultant, Services, Engineering, Process Control, Workplace, Plant, Facilities, Fabrication, Office, Maintenance, Logistics, Supply Chain, Real Estate, Design, Manufacturing

Information and systems you own, manage, or use

- Intellectual property
- Plans, diagrams and schematics
- Physical control systems
- Supervisory Control and Data Acquisition (SCADA) systems
- Building management systems (BMS)
- Physical security systems

The role of Facilities, Physical Systems, and Operations in cybersecurity is all about:

1. Protecting the uniqueness of the products and services that your organization delivers
2. Securing physical systems from compromise
3. Integrating cybersecurity with physical safety and security

What Facilities, Physical Systems, and Operations professionals should do:

- Identify cyber risks to the resilience of physical systems, including control systems
  - » Engage IT and OT stakeholders
  - » Engage trusted third parties to develop an understanding of cyber risks in the physical environment
  - » Perform a comprehensive assessment of the physical environment to identify vulnerabilities and weaknesses
- Develop a comprehensive plan to improve the security of control systems
  - » Leverage cybersecurity best practice frameworks, maintained by authoritative entities such as National Institute of Standards and Technology (NIST), Center for Internet Security (CIS), International Organization for Standardization (ISO)
- Incorporate cybersecurity measures into the safety program
  - » Ensure employee training includes awareness of cyber risks in the physical environment
  - » Leverage the safety program as another means to foster a cyber-secure culture
  - » Partner with IT to develop a system for guests who access the physical environment: limiting direct access, providing a restricted Wi-Fi network, etc.
- Protect intellectual property
  - » Use encryption, passwords, and other methods to secure files when you transfer them to/from customers and partners
  - » Share only necessary information
  - » Ensure sensitive information is destroyed in compliance with the organization's data retention policies or external regulations
  - » Prevent remote access to systems unless absolutely necessary
- Protect access to your information repositories by applying best practices, such as:
  - » Strong, complex passphrases

- » Unique passphrases for each critical account
- » Multi-factor authentication

What we all should do:

- Use social media wisely
  - » Apply strong privacy settings
  - » Don't share personal information on business accounts
  - » Don't share business information on personal accounts
- When working from home, secure your home network by applying best practices (see NIST SP 800-46 Rev. 2), such as:
  - » Change your wireless router SSID and password from the default or "out of the box" settings
  - » Change the password frequently and monitor connected devices
  - » Maximize encryption levels on your wireless router
  - » Increase privacy settings on your browser
  - » Use VPN to access corporate networks whenever possible
  - » For additional security, protect browsing privacy through encrypted browsers
  - » For additional security, protect personal email accounts through encrypted email
- When traveling, secure your connections back to the enterprise
  - » Use VPN access to corporate networks whenever possible
  - » Do not enter sensitive information on public computers
  - » Do not use public Wi-Fi without VPN
  - » Use a dedicated wireless hotspot for internet access
  - » If a hotspot is not available, consider tethering to an issued cell phone
  - » Physically protect your computer from theft and unauthorized access

A note to leaders:

Cultural barriers are as big as any other factor when it comes to cybersecurity in industrial environments and physical systems. It will require persistence, education, and leadership by example to build bridges between operational technology and information technology professionals, as well as between cybersecurity and industrial safety advocates.

Address risks holistically, across all domains. Insist that your employees do the same. Just as safety culture is driven by good leadership, sound performance management, and effective training, so is cybersecurity culture in operational environments.

Finance and Administration

Providing planning, forecasting, accounting, transactional and administrative support to all functions within the organization

What Finance and Administration does

If you are involved in managing the organization's finances, from planning and budgeting to accounting and transactions through risk management, this section applies to you. You are responsible for ensuring that each part of the organization has the ability to pay for goods and services, operate within a budget, track revenues and expenditures, and conduct business with external entities—from customers to suppliers. You may also provide administrative support to the Planning and Governance function or manage office operations. While this function includes all persons with a full-time role in these areas, it also applies to all executives, managers, and associates who handle financial and administrative matters; in other words, just about everyone.

In many cases, the Finance and Administration function includes enterprise risk management, with associated processes and personnel reporting into a Chief Finance Officer (CFO) or similar role. Internal audit and compliance functions may also be included.

You matter to the organization because nothing can happen without the ability to maintain financial health, perform essential transactions, manage business risks and support the Planning and Governance function.

The role of Finance and Administration in cybersecurity is all about:

1. Integrating cyber risks into the enterprise risk management process
2. Resourcing cybersecurity initiatives consistent with security strategy, and balanced with other IT investments
3. Maintaining the confidentiality and integrity of sensitive financial information to ensure security and compliance with applicable policies

What Finance and Administration professionals should do:

- Ensure that cyber risks are integrated into the enterprise risk management process
  - » Identify cyber-related risks to the enterprise early in the risk management process, not as a separate activity or late addition
  - » Understand the many different business effects of cyber threats, which range from business disruption and loss of credibility to legal liability and physical damage
- Provide sufficient funding to enable the success of the organization's cybersecurity strategy
  - » Reference the organization's security strategy and external best practice frameworks to help prioritize investments
  - » Work with cybersecurity leaders to understand how their resource requests align with strategy (which, in turn, should align with enterprise risk management); differentiate between the must-haves and nice-to-haves
  - » Develop a complete view of security-related spending, which is often spread across multiple functional areas and budget allocations
- Collaborate and work on a strategy for emergency cybersecurity spending
  - » In the event of a cyber incident, incident response plans should also incorporate how to purchase needed equipment or services
  - » Vendors and contractors should already be vetted and in place if such an incident should occur
  - » Contingency plans should be made for loss of financial systems to ensure continuity with minimal disruption

Your title includes words like…

Finance, Financial, Comptroller, Accountant, Budget, Risk, Compliance, Contracting, Purchasing, Procurement, Vendor Management, Auditor, Examiner, Loan, Trader, Underwriter

Information and systems you own, manage, or use

- Financial performance records
- Budgets
- Financial assessments and audit reports
- Tax filings (e.g. IRS forms)
- Public files (e.g. SEC forms)
- Planning tools and platforms
- Enterprise risk management tools and platforms
- Risk assessments and audit reports
- Compensation and benefits information
- Accounts payable systems
- Accounts receivable systems
- Contracts

- Work with Legal and Compliance, and Information Technology, to ensure contracts with third parties include clauses for effective oversight of supplier cybersecurity, notification of incidents, and adherence to relevant industry and government policies and regulations
- Define the appropriate balance of resource allocation between run-the-business or improve-the-business and secure-the-business investments
  - » While the former can demonstrate a closer alignment to organization goals and performance, a rush to implement them often introduces new risks
  - » If done properly, improvements in IT operations can also improve security and compliance, since many foundational controls for security (such as asset profiling, vulnerability management, configuration and patch management and access management) are essential to a well-run IT environment
- Protect the organization's financial viability and reputation by ensuring compliance with financial laws, regulations, rules, standards, and policies (both external and internal)
  - » Understand the regulatory requirements associated with financial information, such as Sarbanes-Oxley (SOX), Gramm-Leach-Bliley Act (GLBA) and Payment Card Industry Data Security Standards (PCI DSS)
  - » Support the cybersecurity team's efforts to secure systems which are impacted by these requirements
- Protect sensitive strategic, financial, legal, and risk information
  - » Share only necessary information
  - » Ensure the information is destroyed in compliance with the organization's data retention policies or external regulations
  - » Use encryption, passwords and other methods to secure files when you transfer them to others
- Protect access to any online file sharing or decision support platform by applying best practices, such as:
  - » Strong, complex passphrases
  - » Unique passphrases for each critical account
  - » Multi-factor authentication

What we all should do:

- Use social media wisely
  - » Apply strong privacy settings
  - » Don't share personal information on business accounts
  - » Don't share business information on personal accounts
- When working from home, secure your home network by applying best practices (see NIST SP 800-46 Rev. 2), such as:
  - » Change your wireless router password, SSID, and limit ability of others to find it
  - » Maximize encryption levels on your wireless router
  - » Increase privacy settings on your browser
  - » Use Virtual Private Networks (VPN) to access corporate networks whenever possible
  - » For additional security, protect browsing privacy through encrypted browsers
  - » For additional security, protect personal email accounts through encrypted email
- When traveling, secure your connections back to the enterprise:
  - » Use VPN access to corporate networks whenever possible
  - » Do not enter sensitive information on public computers
  - » Do not use public Wi-Fi without VPN
  - » Use a dedicated wireless hotspot for internet access
  - » If a hotspot is not available, consider tethering to an issued cell phone
  - » Physically protect your computer from theft and unauthorized access

A note to leaders:

As Finance and Administration leaders, you are often the default arbiter for resource demands among the other business functions. At the same time, there are many decisions that must be influenced or made by you in organizational planning, enterprise risk management, and resource allocation in which you are not the subject matter expert—but the decisions must be made.

Get smart about cybersecurity and enterprise risk. Your job, and the financial health of the organization, depends on your ability to make reasonable recommendations and decisions where there are many trade-offs.

Human Resources

Planning, hiring, and supporting the development, retention, and compensation of the organization's workforce

What Human Resources does

If you are responsible for the management and optimization of the organization's human resources—from entry-level staff to senior executives—as well as external stakeholders—from job candidates to recruiters, consultants, human resources associations, and benefits providers—this applies to you. You are responsible for human resource strategy in alignment with the overall strategy of the organization, and serve as subject matter experts in the areas of human resources policies and management, talent acquisition and development, workforce and succession planning, employee relations and engagement, culture and diversity, performance management, and compensation and benefits. You may also be involved in maintaining records in platforms such as human resources administration portals and talent acquisition tools.

You matter to the organization, because without your expertise and efforts to acquire, cultivate, and retain the organization's most valuable asset, its people, the organization would not possess the knowledge, skills, and abilities necessary to succeed. Because of you, many hard-learned best practices for human resource management can be applied in a consistent manner.

The role of Human Resources in cybersecurity is all about:

1. Implementing best practices in organizational change management, employee training, and performance management to enable a cyber-secure culture
2. Ensuring that critical cybersecurity roles are filled, consistent with the NICE Cybersecurity Workforce Framework, and that employees remain current on necessary knowledge, skills and abilities
3. Safeguarding sensitive employee information
4. Spearhead efforts to mitigate the risks of insider threat

What Human Resources professionals should do:

- Leverage NIST Special Publication 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework to deploy human resources to the proper cybersecurity roles
  - » Reference this framework for workforce planning, competency development, talent acquisition, and retention
  - » Reference this framework to identify non-cybersecurity-specific roles which can perform cybersecurity functions
  - » Apply standard lexicon to internal planning conversations, to ensure a common understanding across business functions
- Ensure cybersecurity knowledge, skills, and abilities are incorporated into employee training and development programs
- Require and track participation in cybersecurity training and awareness programs for all employees across the enterprise
- Leverage human resources best practices to support retention of critical cybersecurity roles
- Be vigilant to ensure selection of vendors that can effectively maintain the confidentiality of employee personal information, which frequently includes protected health information
- Protect access to your human resource management platform by applying best practices, such as:
  - » Strong, complex passphrases
  - » Unique passphrases for each critical account
  - » Multi-factor authentication
- Protect sensitive information in employee recruiting, performance, compensation, and benefits:
  - » Share only necessary information
  - » Ensure the information is destroyed in compliance with the organization's data retention policies or external regulations
  - » Use encryption, passwords, and other methods to secure files when you transfer them internally, or externally with stakeholders such as recruiters, potential hires, etc.

Your title includes words like…

Human Resources, Human Capital, People, Talent, Recruitment, Acquisition, Labor, Organizational Design, Training, Benefits, Compensation

Information and systems you own, manage, or use

- Employee data
- Human resource information systems
- Recruitment and onboarding systems (applicant tracking systems)
- Performance management systems
- Succession planning models
- Benefits administration systems

What we all should do:

- Use social media wisely:
  - » Apply strong privacy settings
  - » Don't share personal details on business accounts
  - » Don't share business information on personal accounts
- When working from home, secure your home network by applying best practices (see NIST SP 800-46 Rev. 2), such as:
  - » Change your wireless router password, SSID, and limit ability of others to find it
  - » Maximize encryption levels on your wireless router
  - » Increase privacy settings on your browser
  - » Use Virtual Private Networks (VPN) to access corporate networks whenever possible
  - » For additional security, protect browsing privacy through encrypted browsers
  - » For additional security, protect personal email accounts through encrypted email
- When traveling, secure your connections back to the enterprise:
  - » Use VPN access to corporate networks whenever possible
  - » Do not enter sensitive information on public computers
  - » Do not use public Wi-Fi without VPN
  - » Use a dedicated wireless hotspot for internet access
  - » If a hotspot is not available, consider tethering to an issued cell phone
  - » Physically protect your computer from theft and unauthorized access

A note to leaders:

Human resource professionals have always played an important role in addressing business risks, ranging from natural disasters and workplace violence to lawsuits and lay-offs. Cyber-related business risks are no different: they cannot be effectively addressed without the implementation of best practices in workforce management.

Be proactive in working with other business functions to address cyber-related risks. Early involvement is the key to ensuring that the right people are in the right roles, with the right knowledge, skills, and abilities, doing the right things.

Legal and Compliance

Ensuring compliance with laws, regulations and standards, mitigating risk, and addressing legal matters

What Legal and Compliance does

If you are focused on mitigating or responding to legal risks or compliance matters, this applies to you. You do this in large part by ensuring that the organization remains compliant with the numerous laws, regulations, and standards that apply to it. You may also respond to external inquiries, challenges or complaints, as well as internal matters of a sensitive nature.

You are close advisors to senior leaders, helping to set policies and priorities in a manner that balances the organization's primary purpose with the risks to which it may be exposed. You are highly responsive to legal threats, and may become the focal point of interaction with those outside the organization when legal or compliance matters need to be addressed, such as during litigation, court proceedings, audits, and when law enforcement is involved.

You matter to the organization, because you ensure that it remains in good standing with laws, regulations and standards, allowing it to focus on its core competencies. Without you, the organization could easily find itself in trouble, and subject to criminal, civil and audit liabilities.

Your title includes words like…

General Counsel, Corporate Counsel, Inspector General, Internal Audit, Legal, Compliance, Risk, Privacy Officer, Attorney, Investigator, Paralegal, Legal Assistant, Import/Export Compliance

Information and systems you own, manage, or use

- Articles of incorporation, charters and formation documents
- Contracts and agreements
- Compliance reports
- Audit reports
- Legal briefs
- Communications with retained law firms
- Communications with law enforcement agencies
- Databases and file storage for Legal and Compliance teams

The role of Legal and Compliance in cybersecurity is all about:

1. Minimizing liabilities associated with the organization's cybersecurity posture
2. Ensuring compliance with cybersecurity laws, regulations, and standards
3. Addressing the legal implications of incidents when they arise

What Legal and Compliance professionals should do:

- Understand the legal implications of cybersecurity in order to enable sound risk mitigation
  - » Engage with credible third parties to learn about cybersecurity and law—this includes professional associations, industry groups, consultants, and educators
  - » Remain current on emerging regulations and standards
- Implement an effective compliance program for the organization
  - » Assess the organization's exposure to laws, regulations, and industry standards to ensure appropriate coverage
  - » Leverage existing best practices for compliance enforcement
  - » Ensure third-parties adhere to organizational cybersecurity policies through contractual terms, such as Service-Level Agreements (SLAs)
- Actively participate in the enterprise risk management process, working with Planning and Governance, Finance and Administration, and other business functions to mitigate risks in a holistic manner
- Actively support the organization's incident responders during a suspected breach
- Conduct post-incident law enforcement engagement, vendor notifications and public notifications as required
- Protect access to any online file sharing or decision support platform by applying best practices, such as:
  - » Strong, complex passphrases
  - » Unique passphrases for each critical account
  - » Multi-factor authentication
- Protect sensitive legal and compliance information
  - » Share only necessary information
  - » Ensure the information is destroyed in compliance with the organization's data retention policies or external regulations
  - » Use encryption, passwords, and other methods to

secure files when you transfer them to others

- Lead the organization's efforts to develop and implement privacy guidelines consistent with applicable laws, industry regulations, and best practices

What we all should do:

- Use social media wisely
  - » Apply strong privacy settings
  - » Don't share personal information on business accounts
  - » Don't share business information on personal accounts
- When working from home, secure your home network by applying best practices (see NIST SP 800-46 Rev. 2), such as:
  - » Change your wireless router password, SSID, and limit ability of others to find it
  - » Maximize encryption levels on your wireless router
  - » Increase privacy settings on your browser
  - » Use Virtual Private Networks (VPN) to access corporate networks whenever possible
  - » For additional security, protect browsing privacy through encrypted browsers
  - » For additional security, protect personal email accounts through encrypted email
- When traveling, secure your connections back to the enterprise:
  - » Use VPN access to corporate networks whenever possible
  - » Do not enter sensitive information on public computers
  - » Do not use public Wi-Fi without VPN
  - » Use a dedicated wireless hotspot for internet access
  - » If a hotspot is not available, consider tethering to an issued cell phone
  - » Physically protect your computer from theft and unauthorized access

A note to leaders:

No matter how many cybersecurity professionals are hired, or how much investment is made in mitigating tools and technologies, the organization will not be able to adequately address cyber-related risks until the legal implications are considered. Furthermore, the organization could improve security but still be exposed to liability due to non-compliance. Work with cybersecurity experts, as well as legal advisors, auditors, and consultants, to ensure that exposure is minimized and the organization can focus on its mission.

Ask the difficult questions. Your colleagues may not be asking the right questions, or may be avoiding addressing the hard ones. They may be ignoring the requests of cybersecurity professionals within the organization. But chances are, they will listen to you.

Information Technology

Leveraging technology solutions for business connectivity, productivity, and essential processes

What Information Technology does

If you define, develop, test, deploy, support, maintain, and protect technology solutions for the organization, this applies to you. You are responsible for the "central nervous system" of the business, managing the computing systems and networks that enable decision making and communication, and then translating that content into processes that run the business. You are likely involved in interacting with end users to gather and deliver to their requirements. You may interact closely with the Human Resources and Legal and Compliance functions to ensure organization-wide awareness of, and adherence to, cybersecurity policies. You may also be involved in interacting with external vendors for technology acquisition and support. In the event of a cybersecurity incident, you would likely interact with service providers, law enforcement, and external cybersecurity organizations.

You matter to the organization, because you enable everyone to communicate, capture data, process information, and manage the systems that work depends on. Critical assets, including confidential information, intellectual property, competitive differentiators, and customer data, can be properly used and protected because of your role.

Your title includes words like…

Technology, Information, IT, Infosec, Cybersecurity, Data, Systems, Computer, Network, Telecommunications, Database, Business Process, Software, Coding, Programmer, Web, Red Team, Blue Team

Information and systems you own, manage, or use

- Privileged accounts
- Access controls to critical systems
- Active Directory and associated personnel information
- Results of cybersecurity assessments, audits and penetration tests
- Internal infrastructure, from servers and storage systems to network devices and endpoint systems
- Externally-hosted (cloud-hosted) platforms and data

The role of Information Technology in cybersecurity is all about:

1. Providing technical expertise for the security of information systems and associated technology platforms
2. Implementing and maintaining a robust multi-layered (defense-in-depth) approach to the organization's information security, consistent with industry best practices and compliant with applicable regulations and standards
3. Responding to and mitigating security-related incidents

What Information Technology professionals should do:

- Provide technical expertise in support of the organization's cybersecurity program
  - » Ensure current knowledge in cybersecurity tools, techniques, and procedures
  - » Cross-train other IT roles with security functions in order to develop a broader awareness of, and capacity to implement, cybersecurity best practices
  - » Collaborate proactively with other business functions across the enterprise
- Implement a robust cybersecurity program, with appropriate technical and process controls consistent with the organization's risk mitigation strategy
  - » Leverage cybersecurity best practice frameworks, maintained by authoritative entities such as the National Institute of Standards and Technology (NIST), Center for Internet Security (CIS), and International Organization for Standardization (ISO)
  - » Work with external entities, such as consultants, auditors, professional associations and product and service providers to identify the best tools for the job
- Integrate security into IT design, architecture, deployment and routine operations
  - » Consider security upfront, not as an afterthought
  - » Integrate security throughout the application development, testing, staging, and deployment process, including DevOps
  - » Leverage IT operational best practices to improve security
- Establish and enforce robust security policies for employees, contractors, and vendors
- Establish, verify, and enforce robust cloud security policies for the organization
  - » Ensure that cloud service providers deliver the level of security that the organization requires

  - » Understand the shared responsibility models associated with consumption of cloud services
  - » Establish and enforce internal security policies for use of cloud services
- Protect access to any online file sharing or decision support platform by applying best practices, such as:
  - » Strong, complex passphrases
  - » Unique passphrases for each critical account
  - » Multi-factor authentication
  - » Use of password manager systems or applications
- Protect sensitive organizational information
  - » Share only necessary information
  - » Ensure the information is destroyed in compliance with the organization's data retention policies or external regulations
  - » Use encryption, passwords, and other methods to secure files when you transfer them to others
  - » Use encryption, passwords, and other methods to secure files at rest
  - » Ensure redundant storage of critical information
- Maintain a high degree of technical competence in Knowledge, Skills, and Abilities (KSAs) essential to cybersecurity
  - » Actively participate in professional associations, conferences, and events
  - » Pursue formal education in relevant fields
  - » Achieve technical certifications in cybersecurity domains
  - » Continue to hone skills and demonstrate mastery through participation in cybersecurity competitions

What we all should do:

- Use social media wisely
  - » Apply strong privacy settings
  - » Don't share personal information on business accounts
  - » Don't share business information on personal accounts
- When working from home, secure your home network by applying best practices (see NIST SP 800-46 Rev. 2), such as:
  - » Change your wireless router password, SSID, and limit ability of others to find it
  - » Maximize encryption levels on your wireless router
  - » Increase privacy settings on your browser
  - » Use Virtual Private Networks (VPN) to access corporate networks whenever possible
  - » For additional security, protect browsing privacy through encrypted browsers
  - » For additional security, protect personal email accounts through encrypted email
- When traveling, secure your connections back to the enterprise:
  - » Use VPN access to corporate networks whenever possible
  - » Do not enter sensitive information on public computers
  - » Do not use public Wi-Fi without VPN
  - » Use a dedicated wireless hotspot for internet access
  - » If a hotspot is not available, consider tethering to an issued cell phone
  - » Physically protect your computer from theft and unauthorized access

A note to leaders:

The technical expertise essential to effective cybersecurity resides within your business function. It is imperative that IT professionals, including but not limited to those with cybersecurity roles, have the requisite knowledge, skills, and abilities to perform their roles. This means continuous education, training, and certification to stay current in a dynamic field.

Keep your skills sharp. Ensure that you and your team members are able to address the complexities of the field, respond quickly to emerging threats, and answer difficult technical questions. Your credibility and performance depend on it!

Appendix 1: Doing the Right Things

The following are guidelines for all individuals—as citizens, consumers and employees—regardless of business function, to avoid becoming "Patient Zero"

When organizations become the victim of a cybersecurity breach, especially in phishing-related attacks, those investigating how the exploit entered their organization seek to find "Patient Zero." This is a term adopted from medical forensics, and is used to identify the person or group that was the entry point for a malicious exploitation into their information technology environment.

While multi-layered security protections are important, particularly if implemented in an automated fashion, the organization is still relying on individuals to *do the right things*.

Individuals across many levels of an organization have damaged their organization's brand and reputation, and even lost their jobs or ruined their careers when cyber exploitations have occurred. The obvious question for personnel in these organizations is "What should I do to avoid becoming 'Patient Zero'?" What everyone should do is, in a general sense, straightforward: become more cyber-aware and exercise better cyber hygiene.

In the context of an organization's business and technology environment, those organizations wanting to create a robust cybersecurity culture for their organization must implement good cybersecurity practices to mitigate their critical cybersecurity risks. Most important is communicating and helping everyone in the organization know and understand what those in the organization and their partners are expected to do. To be successful in this area, this cannot be a one-time awareness or training event, but a continuous effort to make everyone aware of current cyber-related risks and the practices their organization expects each person will perform.

As a general rule, every individual in an organization should be performing the following common tasks:

- **Exercise caution** when using information systems; if you are unsure or sense you may be doing something risky, seek guidance from responsible individuals
- **Fully understand your role** and take personal responsibility for knowing how your organization addresses cybersecurity risks
- **Know how to handle, control, store, transfer and dispose of information** in your organization
- **Protect your assets by** safeguarding your computer and mobile devices
- F**ollow your organization's security procedures** for facilities and prevent unauthorized access via social engineering tricks
- **Use the best authentication capabilities your organization offers** for controlling access to computers, mobile devices and the information services and applications you use
- **Use encryption** for information in transit and at rest
- **If you work from home, secure your home devices and connections**
- **If you travel, know how your organization wants you to secure your connections** back to the organization through public networks
- **Know your organization's policies and practices for using personal devices for work**
- **Know your organization's security incident reporting policy and contacts**

Appendix 2: Authors and Contributors

Names are followed by professional titles and affiliated organizations. Roles specific to this project are denoted in (parentheses)

Editors and Project Leaders

Susie Cone, IT Consultant (Editor, Co-Chair, Workforce Management, NICE Working Group)

Pilar Jarrin, Manager, Deloitte Consulting LLP (Co-Facilitator)

Kristin Judge, CEO & President, Cybercrime Support Network (Co-Chair, Workforce Management, NICE Working Group)

Rachel Mastro, Human Capital Consultant, Deloitte Consulting LLP (Co-Facilitator)

Maurice Uenuma, Strategic Engagements, Tripwire (Project Lead; Editor; Co-Chair, Workforce Management, NICE Working Group)

Stephen Woskov, Senior Consultant, Deloitte Consulting LLP (Co-Facilitator)

Authors

Tanya Brewer, Project Manager, National Institute of Standards and Technology

Roger Callahan, Managing Director, Information Assurance Advisory, LLC

Susie Cone, IT Consultant (Editor, Co-Chair, Workforce Management, NICE Working Group)

Lori Gordon, Senior Strategist, HWC Inc.

Kristin Judge, CEO & President, Cybercrime Support Network (Co-Chair, Workforce Management, NICE Working Group)

Charmaine Sheeler-Mitchell, Occupation Safety and Health Review Commission

Maurice Uenuma, Strategic Engagements, Tripwire (Project Lead; Editor; Co-Chair, Workforce Management, NICE Working Group)

Contributors and Reviewers

Nancy Austin, Leonardo Coaching

Steven Aude, Ph.D., Vice President, ICF

Steven Bledsoe, Principal, Z-Rated.com Inc.

Chris Burns, Information Security Manager, General Motors

Roger Callahan, Managing Director, Information Assurance Advisory, LLC

Veronica Colon, VP, STEM Outreach

Karl Cureton, Executive Chairman, The National Minority Technology Council

Robin Drake, Program Associate, National Initiative for Cybersecurity Education (NICE)

Susan Hansche, CDM Training Manager, U.S. Department of Homeland Security

Katie Hanson, Director of Communications, US Cyber Challenge

James Harris, Vice President, PFP Cybersecurity

Laura Hatzes, Program Associate, National Initiative for Cybersecurity Education (NICE)

Jason Hite, Founder & Chief People Strategist, Daoine Centric LLC (Industry Co-Chair, NICE Working Group)

Rita Heimes, J.D., Research Director and Data Protection Officer, International Association of Privacy Professionals

Carol Hodes, Ph.D, Senior Consultant, NOCTI

Hillary Homan, Workforce Development and Change Management SME - Nodi Solutions, LLC

Pilar Jarrin, Manager, Deloitte Consulting LLP (Co-Facilitator)

Kevin Johnson, Manager, Cybersecurity Audit and Compliance, National Cancer Institute, National Institutes of Health (NIH)

Ron Kantor, Ph.D., Learning and Development Consultant

Tom Klemas, Principal Engineer, SimSpace Corporation

Mark Kosier, CIO, Tech + Equation, Inc.

Noel Kyle, Cybersecurity Education and Awareness Branch, U.S. Department of Homeland Security

David Martinez, Vice President, Operations, The Partnership Federal Credit Union

Rachel Mastro, Human Capital Consultant, Deloitte Consulting LLP (Co-Facilitator)

Peter Meehan, iQ4 Corp, Co-Founder Cybersecurity Workforce Alliance (CWA)

Marian Merritt, Lead for Industry Engagement, National Initiative for Cybersecurity Education (NICE)

Paul Montrose, Principal Information Security Manager, Acxiom Corporation

Bill Newhouse, Deputy Director, National Initiative for Cybersecurity Education (NICE)

Erika Olsen, Senior Legal Counsel, Public Safety & Homeland Security Bureau, Federal Communications Commission

Murielle Palmier, Development & Partnership Director, ASPertise

Celia Paulsen, Acting Coordinator for Industry Engagement, National Initiative for Cybersecurity Education (NICE)

Vince Peeler, CEO/Founder, Enlighten Cyber Security Training

Rodney Petersen, J.D., Director, National Initiative for Cybersecurity Education (NICE)

Evelyn Petrella, Program Associate, National Initiative for Cybersecurity Education (NICE)

Damira Pon, Director of Student Services, Digital Forensics Program, University at Albany, State University of New York

MaryAnn Pranke, President, MPT&C Inc.

Portia Pusey, Ed.D., Consultant

James Rensimer, Managing Partner, The Rensimer Law Firm

Paul Ricketts, Nuclear Regulatory Commission

Mike Riley, Program Manager, U.S. Department of State

Kevin Sanchez-Cherry, Cybersecurity Policy, Architecture and Training Lead, U.S. Dept. of Transportation

Danielle Santos, Program Manager, National Initiative for Cybersecurity Education (NICE)

Sondra Schneider, President, Security University

Paul Schwartz, Director of Information Security, Lansing Community College

Benjamin Scribner, Section Chief, Outreach, U.S. Department of Homeland Security CS&C/SECIR/CE&A

David Shaheen, Information Security Forensics Lead, Henry Ford Health System

Rebecca Slayton, Ph.D., Associate Professor, Cornell University

James Stanger, Chief Technology Evangelist, CompTIA

Julie Steinke, Ph.D., Lead Behavioral Scientist, MITRE Corporation

Charlie Tupitza, CEO, Global Forum to Advance Cyber Resilience

Frederic Vezon, President, ASPertise

Ping Wang, Ph.D., Professor of Computer and Information Systems, Robert Morris University

Alan Watkins, ABW Consulting Services / ABW InfoSec Consulting; Core Adjunct Professor, Cyber Security & Information Assurance, National University, School of Engineering & Computing

Greg White, Ph.D., Executive Director, ISAO Standards Organization, University of Texas at San Antonio

Dana Winner, President, Dana Winner, Inc.

Stephen Woskov, Senior Consultant, Deloitte Consulting LLP (Co-Facilitator)

Creative Design

Harold Metzger, Creative Services Manager, Tripwire

Appendix 3: Methodology

The recommendations provided in this publication reflect the input of numerous contributors across a variety of industries, roles and backgrounds. From the outset, the intention has been to provide a carefully-curated, distilled set of guidelines that are readily understandable and applicable to those who may be new to cyber-related risks, and which provides a comprehensive, enterprise-wide view of how everyone has a role to play in the security of the organization.

To that end, the following steps were taken to ensure that many voices were heard and a broad set of perspectives considered:

- A new subgroup was formed under the National Initiative for Cybersecurity Education (NICE) Working Group:
  - » During May of 2016, the NICE Working Group merged two subgroups: Career Development and Workforce Planning, and Workforce Framework. The newly formed subgroup, Workforce Management, came together to develop a charter outlining goals and objectives and clarifying scope. A decision was made to focus on the enterprise side of workforce management risk and human risk for all levels of an organization.
  - » The newly formed Workforce Management subgroup began with just over 40 members. By December 2017, membership grew to nearly 100 members, and has grown to over 150 participants by May 2018.
- A project to develop guidelines was scoped:
  - » The need for this guidebook was identified by the Workforce Management subgroup. The decision to focus mainly on the demand (or employer) side of the labor market is a unique aspect of this subgroup's work within the context of the NICE Working Group.
  - » Specific goals for the guidebook stemmed from discussions on the NICE Cybersecurity Workforce Framework and the belief that everyone has a role in cybersecurity, no matter the position.
- A literature review was performed by a team of seven, and gathered 28 relevant resources during the early months of 2017. These resources were read and summarized for use by the broader project team.
- A reference framework was developed by May 2017 to map out the various common functions essential to organizations:
  - » The group outlined business functions and components to frame a holistic view of organizations.
  - » The group identified potential impacts if cyber-related risks were not properly addressed.
- Deep-dive sessions were held during the summer and autumn months of 2017 to develop guidelines for each business function:
  - » Seven sessions were held, involving a total of 12 contributors.
  - » Over the course of three months, members met as smaller groups to examine all business functions and roles in an organization and how they contribute to and mitigate cybersecurity risk, integrating business, cybersecurity, and human resources disciplines. Discussions considered different levels of personnel including executive leadership, middle management, and individual contributors, and examined the risk of not performing a role as well as mitigation strategies.
- Based on the guidelines developed during the deep-dive sessions, individual sections for each business function were drafted by the Authors in late 2017 and early 2018, along with introductory content and appendices.
- These sections were included in the first complete draft, which was reviewed by the Workforce Management Sub-Group in February 2018:
  - » Members of the Sub-Group were requested to individually review the draft, and submit comments and suggested edits.
  - » The input of Contributors and Reviewers was consolidated into the draft, which was then reviewed by the Editors.
  - » The updated draft was submitted to the broader NICE Working Group for review on February 28, 2018.
- The broader NICE Working Group reviewed and commented on the draft by March 23, 2018
  - » Numerous individuals provided comments, as noted in Appendix 1.
  - » Again, the input of NICE Working Group Contributors and Reviewers was consolidated into the next draft by the Editors.
- The near-final version of the guidebook, prepared for public comment, was completed on June, 2018 and made available to the public on July, 2018.
  - » This version included new graphic design, contributed by Tripwire.
- Final publication process [pending]

Appendix 4: Where to Learn More

Given the brief and distilled nature of this publication, this section is intended to provide additional resources on the many subject areas introduced in the preceding pages.

This is not an exhaustive list, and the presence, or lack thereof, of any particular organization or its resources does not constitute an endorsement or a validation of its content, but does reflect the general consensus of the authors, contributors and reviews regarding the relevance of the sources to the goal of a cyber-secure workforce.

Government departments and agencies:

- National Institute of Standards and Technology (NIST), at https://www.nist.gov/
  - » Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework), at https://www.nist.gov/cyberframework
  - » National Initiative for Cybersecurity Education (NICE), at https://www.nist.gov/itl/applied-cybersecurity/national-initiative-cybersecurity-education-nice
  - » NICE Cybersecurity Workforce Framework (NCWF), at https://www.nist.gov/itl/applied-cybersecurity/national-initiative-cybersecurity-education-nice/nice-cybersecurity
  - » Password guidance, at https://www.nist.gov/video/password-guidance-nist-0
  - » NIST SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, at https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final
- U.S. Department of Energy, at https://www.energy.gov/
  - » Cybersecurity Capability Maturity Model (C2M2) Program, at https://www.energy.gov/oe/cybersecurity-critical-energy-infrastructure/cybersecurity-capability-maturity-model-c2m2-program
- U.S. Department of Homeland Security (DHS), at https://www.dhs.gov/
  - » U.S. Computer Emergency Readiness Team (US-CERT), at https://www.us-cert.gov/
  - » National Initiative for Cybersecurity Careers and Studies (NICCS), at https://niccs.us-cert.gov/
  - » Cybersecurity Workforce Development Toolkit, at https://niccs.us-cert.gov/workforce-development/cybersecurity-workforce-development-toolkit
  - » Federal Virtual Training Environment, at https://fedvte.usalearning.gov/
  - » Nuclear Sector Cybersecurity Framework Guidance for U.S. Nuclear Power Reactors, at https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/nuclear-framework-implementation-guide-2015-508.pdf
- National Security Agency (NSA), at https://www.nsa.gov/
  - » National Centers of Academic Excellence in Cyber Defense, at https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/
- Federal Bureau of Investigation (FBI), at https://www.fbi.gov/
  - » InfraGuard, at https://www.infragard.org/
- U.S. Secret Service (USSS), at https://www.secretservice.gov/
  - » Cyber crimes investigation, at https://www.secretservice.gov/investigation/#cyber
- U.S. Defense Information Systems Agency (DISA), at https://www.disa.mil/
  - » Cyber Crimes Investigations, at https://www.secretservice.gov/investigation/#cyber
- U.S. Federal Trade Commission, at https://www.ftc.gov/
  - » OnGuard Online, at https://www.ftc.gov/news-events/audio-video/consumers/onguard-online
- U.S. Nuclear Regulatory Commission, at https://www.nrc.gov/
  - » Regulatory Guide 5.71 Cyber Security Programs for Nuclear Facilities, at https://www.nrc.gov/docs/ML0903/ML090340159.pdf

Standards organizations and non-profit entities:

- Center for Internet Security (CIS), at https://www.cisecurity.org/
  - » CIS Critical Security Controls, at https://www.cisecurity.org/controls/
- International Organization for Standardization (ISO), at https://www.iso.org/home.html
  - » ISO/DIS 30401 Knowledge Management Systems - Requirements, at https://www.iso.org/standard/68683.html
  - » ISO 31000 – Risk Management, at https://www.iso.org/iso-31000-risk-management.html
- Information Technology Infrastructure Library (ITIL), at https://www.axelos.com/best-practice-solutions/itil
- National Cyber Security Alliance (NCSA), at https://staysafeonline.org/
  - » Stop.Think.Connect., at https://www.stopthinkconnect.org/
- Online Trust Alliance (OTA), at https://otalliance.org/

Professional associations and training and certification providers:

- Computing Technology Industry Association (CompTIA), at https://www.comptia.org/
- International Council of E-Commerce Consultants (EC-Council), at https://www.eccouncil.org/
- International Information Systems Security Certification Consortium ((ISC)2), at https://www.isc2.org/
- ISACA, at https://www.isaca.org/pages/default.aspx
  - » Control Objectives for Information and Related Technologies (COBIT), at https://cobitonline.isaca.org/
- SANS Institute (SANS), at https://www.sans.org/
  - » Global Information Assurance Certifications (GIAC), at https://www.giac.org/
- International Association of Privacy Professionals (IAPP), at https://iapp.org/
- National Association of Corporate Directors (NACD), at https://www.nacdonline.org/
- Women in Cybersecurity (WiCyS), at https://www.wicys.net/
- National Cybersecurity Student Association, at https://www.cyberstudents.org/
- Minority Cyber Inclusion Council (MCI Council), at http://www.mcicouncil.org/

Cybersecurity product and service providers:

- AT&T, at https://www.business.att.com/solutions/Portfolio/cybersecurity/
- Dell EMC, at https://www.dellemc.com/en-us/data-protection/solutions.htm#dropdown0=0
- Deloitte Consulting LLP, at https://www2.deloitte.com/cy/en/pages/risk/solutions/cyber-security-services.html
- FireEye, at https://www.fireeye.com/blog.html
- Hewlett Packard Enterprise, at https://www.hpe.com/us/en/services/consulting/security.html
- IBM, at https://www.ibm.com/security
- Intel, at https://www.intel.com/content/www/us/en/security/hardware/hardware-security-overview.html
- Qualys, at https://blog.qualys.com/
- Symantec, at https://www.symantec.com/blogs/
- Tripwire, at https://www.tripwire.com/state-of-security/
- Verizon, at http://www.verizonenterprise.com/products/security/

Related resources:

- Carnegie Mellon CyLab Security and Privacy Institute at https://www.cylab.cmu.edu/
- Cybersecurity Workforce Alliance, at http://www.iq4.com/
- Cybersecurity Workforce Handbook, Council on CyberSecurity, at http://pellcenter.org/cyber-leadership/
- CyberCompEx, at https://www.cybercompex.org/
- HR Professional's Guide to a Cyber-Secure Workforce, Council on CyberSecurity, at http://iaadvisory.info/wp-content/uploads/2016/02/HR-Professionals-Guide-to-a-Cyber-Secure-Workforce.pdf
- Purdue Enterprise Reference Architecture, at https://en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture
- Reference ISA-99/IEC-62443 for standards on industrial cybersecurity
- US Cyber Challenge, at https://www.uscyberchallenge.org/