Effective Reporting to the BoD on Critical Assets, Cyberthreats and Key Controls

The Qualitative and Quantitative Model

Cyberrisk is not just an IT issue; it is much broader. The magnitude or impact of a cyberattack can determine the survival of an enterprise. Business risk continues to exist. Executive management is accountable to the shareholders, and the board of directors (BoD) has the fiduciary duty to ensure that internal controls are in place to assess the potential cyberrisk, thwart any cyberthreats and invoke mitigation action in response to cyberattacks.

There is a cultural gap between cybersecurity professionals, BoDs and enterprise executive teams due to the background and traditional focus of each party. Bridging that gap is a two-way street.

The cybersecurity team, led by the chief information security officer (CISO), needs to realize that it is supporting the enterprise's business by aligning the cybersecurity posture with enterprise priorities.

In addition, the BoD and enterprise executives must realize that the CISO should be a professional with C-level traits. The position should not be downgraded to that of a cyberanalyst or a professional with superior technical competency.

According to a survey by the US New York Stock Exchange (NYSE), 66 percent of directors neither believe that their enterprises are properly protected nor are confident that their enterprises could effectively prevent a cyberattack.[1]

According to one report, 53 percent of executives have a strong preference for qualitative information such as recent cybersecurity risk and how well information is secured. In addition, 38 percent of BoDs have a strong preference for quantitative information, such as what is the significant cyberrisk and its impact from the previous quarter, and how is return on investment (ROI) for cyberinitiatives measured.[2] For BODs to make appropriate decisions, qualitative information should be put in context to support quantitative information.

Another interesting result of the same report shows that:[3]

- Only two in five respondents indicate that the information they provide to the board is actionable.

Robert Putrus, CISM, CFE, PE, PMP
Is an information risk officer. He is a seasoned professional with 25 years of experience in cybersecurity, information systems, compliance services, program management and management of professional service organizations. Putrus is experienced in the deployment of various cybersecurity frameworks/standards. He has written numerous articles and white papers in professional journals, some of which have been translated into several languages. Putrus is quoted in publications, articles and books, including those used in Master of Business Administration programs in the United States. He can be reached at robertputrus@therobertsglobal.com and *linkedin.com/in/robert-putrus-8793256*.

> A CISO WITH A TECHNICAL BACKGROUND MAY RELY TOO HEAVILY ON CYBERSTANDARDS AND TRY TO COVER EVERY ASPECT OF RISK FROM SMALL TO LARGE.

- Only one-third of IT and security executives believe that the board understands the information about cybersecurity threats that is provided to it.

The BoD acknowledges that risk cannot be completely eliminated. However, board members would like to know the residual risk for any critical assets to deem as acceptable risk appetite.

Because the BoD is responsible for overseeing the management of an enterprise, any cyberreport to the BoD should articulate key interests of the BoD, such as enterprise risk exposure, sources and nature of threats, risk imposed by the third-party vendors, residual risk, and the appropriate spending level on cybersecurity.

It is the CISO's responsibility to present cyberrisk information to the BoD and prepare the enterprise to face such threats. This dictates that the enterprise provides a transparent environment that allows the CISO to report security risk in business terms and assist the BoD in comprehending the risk posture of the enterprise.

Shifting the Terms From Cybersecurity to Cyberresilience

Cybersecurity is a necessary but insufficient requirement for enterprises due to the serious consequences that a breach may have on an enterprise and its survival. BoDs and senior executives assume much of the accountability for protecting their enterprises from cyberthreats. They demand that cyberprofessionals design, implement and manage effective controls to ensure continued operation and restoration of the enterprise to its normal state following any major cyberevents. Essentially, BoDs want to transition from cybersecurity to cyberresilience.

Cybersecurity is an endless process of chasing and preventing known attacks, anticipating attacks, monitoring, alerting, patching, remediating and implementing solutions. Cybersecurity is about reacting, and it is impossible to predict the nature, timing and prevention of all possible attacks. It is becoming a maintenance function that trails hackers and other bad actors.[4]

Cyberresilience refers to the ability to constantly deliver intended outcomes despite negative cyberevents. It is keeping business intact through the ability to effectively restore normal operations in the areas of information systems, business functions and supply chain management. In simple terms, it is the return to a normal state with a "soft landing."[5]

Cyber and IT Professionals Lost Their Compass

It is time to scrutinize and re-examine the posture of cybersecurity professionals and their adopted practices in protecting enterprises from cyberthreats. Cyberprofessionals attribute successful cyberattacks to lack of cybersecurity spending, shortage of qualified resources, pitfalls of technology solutions and lack of executives' support. When the dust settles, the enterprise suffers and the cyberprofessionals are held accountable for any successful cyberattacks.

Interviews with executives and data from more than 200 enterprises, technology vendors and public agencies indicated that "large institutions lack the facts processes to make effective decisions about cybersecurity,"[6] and larger cybersecurity expenditures have to be translated to increased cybermaturity.

Because of the technical background of cyberprofessionals, there often is a tendency to put too much emphasis on the technology solution to manage cyberrisk, overlooking the people and processes.

A CISO with a technical background may rely too heavily on cyberstandards and try to cover every aspect of risk from small to large. Over-engineering is

difficult to implement and overwhelming for an enterprise to manage. Technical cyberexperts cannot address their organization's cyberrisk without understanding the commercial and organizational requirements.[7] This leads to overinvestment in technical solutions and underinvestment in the coverage of the entire supply chain and complexity reduction of the environment.

Do the cyberprofessionals have a complete representation of the overall enterprise including computing infrastructure and assets to pinpoint what they are protecting? In other words, do they have inventory of the enterprise assets and have such assets been prioritized based on importance to the enterprise? The shortcomings in this scenario are the lack of prioritizing critical assets and treating all assets equally.

> "THE CISO IS EXPECTED TO BRIDGE CYBERTECHNOLOGY, AS A SUB-SERVANT, TO THE ENTERPRISE BUSINESS REQUIREMENTS."

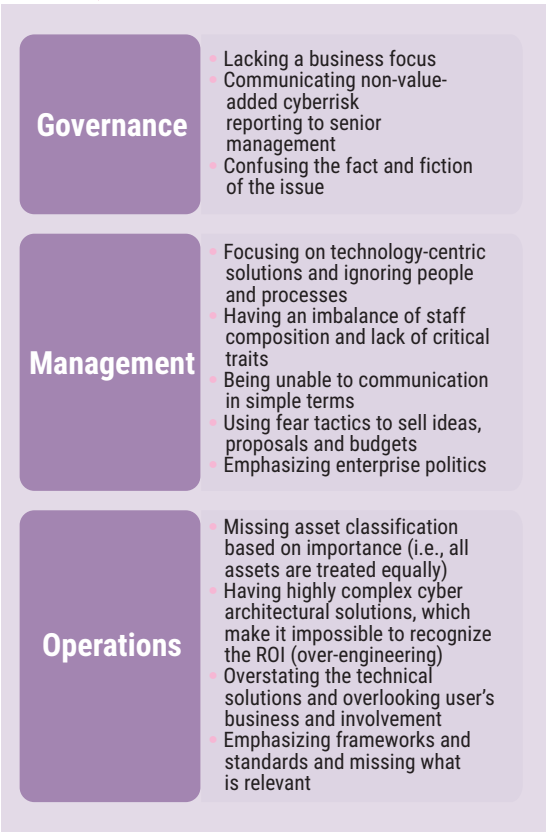
Cyberprofessionals should compile and report on appropriate key performance indicators (KPIs), key risk indicators (KRIs) and key internal controls (KIC). These technical reports and dashboards should be presented to the executive management team and the BoD in ways they can understand, appreciate and on which they can make informed decisions, rather than cyberprofessionals trying to impress BoDs with their technical competencies. BoDs are more interested in knowing how the enterprise is protected from cyberthreats than the cyberprofessionals' technical skills.

It is time for cyberprofessionals to approach cyberrisk planning, management and reporting in precise and meaningful ways. The enterprise is a business, not an IT or cybertechnology testing laboratory.

Cautions From the Failing Phenomena of Cyberresilience Professionals

The maturity and competency of cyber within an organization varies from one enterprise to another. A few weak characteristics are cited in **figure 1**.

Figure 1—Failing Phenomena of Cyberresilience



Communication and Reports of Cyberresilience to the BoD

Cyberrisk and its probable impacts greatly affect an enterprise. BoDs have an increased awareness of it, as evidenced by the fact that the subject is an agenda item in their quarterly and annual meetings. Board members have backgrounds typically in finance, marketing, business, operations and law, with little cyber expertise.

Board members inquire on the health and status of the enterprise, its ability to withstand a cyberattack

> "OFTEN, ENTERPRISES HAVE DIFFICULTY MEASURING HOW SECURE THEIR ASSETS ARE, THE DEGREE OF SECURITY THEY SHOULD HAVE AND HOW MUCH RISK THEY ARE WILLING TO TOLERATE."

and what the enterprise is doing to guard its assets if a cyberincident does occur. In short, board members are looking for assurances on whether the enterprise is properly protected and how risk areas are mitigated.

This is where the CISO's skills as a business professional and facilitator become significant. The CISO is expected to bridge cybertechnology, as a sub-servant, to the enterprise business requirements.

Effective reporting of cyberresilience should articulate the following:

- **Accuracy**—It is correct and represents information on threats and countermeasures taken.
- **Transparency**—It is easily understood by enterprise senior executives to make informed decisions.
- **Classification**—Reporting should be based on asset classification, business function and geography.
- **Quantitative and qualitative**—Reporting should quantify the risk exposure, risk appetite and impacts on the enterprise's financial and legal reputation.
- **Representative**—The report should represent the current risk, threats and controls in place; recommended remediation and expected cost; and tolerated residual risk.
- **Comparative**—It should quantify the risk from previous periods and how it is measured based on industry benchmarks.

Enterprise Assets and Key Controls of the Cyberrisk Model (The Model)

Often, enterprises have difficulty measuring how secure their assets are, the degree of security they should have and how much risk they are willing to tolerate. It is even more complicated to determine how much they are willing to invest to bring risk to an acceptable threshold level.

Risk appetite is highly proportional to the nature of goods and services produced by the enterprise. If the enterprise deals with sensitive and personal information, it will have very low or a no-risk appetite for unauthorized access. As a consequence, these enterprises will invest heavily in tightening certain internal controls. The subjects of risk threshold and risk appetite are likely points of interest, and the measuring of such risk tolerance should be addressed.

The cyberrisk model is partially built from the stated attributes of what could be considered critical assets, threats and key controls.[8] A top-down and bottom-up approach is recommended to mitigate risk from potential threats, with key controls to impede the risk. A combination of quantitative and qualitative approaches should be used when dealing with critical assets.

The cyberrisk model will adopt a quantitative approach that is top down and provides an objective view with the least personal bias. It is based on the prioritization of the enterprise's critical value assets and the impact of the threats on these assets.

Simultaneously, the cyberrisk model will adopt a qualitative approach that is bottom up and will capitalize on the stakeholders' experience based on identifying enterprise key controls in eradicating threats.

The principle of enterprise cyberresilience is to protect assets, identify risk, and identify and deploy key security controls that allow the enterprise to return to a normal state of operation. Furthermore,

the enterprise will continue to run its operations at full capacity with a recovery point and recovery time that has minimal impact on its supply chain.

The cyberrisk model hierarchy and its attributes vary from one enterprise to another. **Figures 2 through 9** can be used to build and examine an enterprise-specific model.

Enterprise Critical Assets

These can be classified as—but are not limited to—human resources (HR), financial, intellectual property (IP), trade secrets, informational, personally identifiable information (PII) or computing environment. The purpose of identifying critical assets is to avoid adverse effects on the enterprise that could occur with the theft, loss, compromise or misuse of those assets. Identification and classification of critical assets are entirely based on the enterprise's rendered services and made products.

Enterprise Security Risk/Threats

One of the compliance requirements with the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standard ISO/IEC 27001 is to identify information assets in order to determine the threats associated with them. The types of risk scenarios and threats enterprise assets could be vulnerable to include physical, people, operational, unsecure software development life cycle (SDLC), third-party relationship risk, network security risk, platform security risk and application security risk.

Enterprise Key Cybersecurity Controls

These are controls based on best practices to be enacted with countermeasures to protect all identified critical cyberassets from compromise. The result is a set of defensible actions to stop and thwart cyberattacks in order to provide confidentiality, integrity and availability of the critical assets.

The Fundamentals of Enterprise Assets

It is time to go back and focus on the fundamentals. Cyberprofessionals should examine and re-engineer how to present enterprise cyberstrategy to their customers: the BoD.

Cyberthreats are directed at people's vulnerabilities, the intellectual assets of data and information, infrastructure architecture defects, and software application flaws. They tend to exploit people, computing devices, network connections, email, communication applications and stored data. The fundamental assets of an enterprise could be summarized in four categories:

1. **Data/information**—Protected information, products, services, patents, financial
2. **People**—Employees, end-users, customers, third parties
3. **Network infrastructure**—Firewalls, switches, servers, load-balancers, intrusion detection systems, web domains, storage devices
4. **Application infrastructure**—Enterprise software or programs, accounting applications, shop-floor management, database programs, email

The scope of the enterprise cyberresilience should be focused and directed on these fundamentals. The fundamentals have intricacies at various degrees of impact on the enterprise cyberresilience that are highly based on the enterprise culture, industry, size and geopolitical stance.

Figure 2—Identified Critical Assets of the Enterprise

Enterprise Assets and Key Controls Cyberrisk Model				
GOAL PROTECT THE ENTERPRISE ASSETS				
CRITICAL ASSETS	Data/Information (35 percent)	People (30 percent)	Network Infrastructure (20 percent)	Application Infrastructure (15 percent)

> ACHIEVING COMPLETE CYBERTHREAT IMMUNITY IS NOT POSSIBLE, AND EVEN IF IT IS ATTEMPTED, IT MAY NOT BE WORTH THE COST.

If cyberprofessionals and IT professionals have a generic cyberresilience focus overlooking how the fundamentals interplay, then they are subjecting their enterprises to eventual cybersecurity breaches.

The new strategy for identifying potential threats should focus on the fundamentals and be revisited periodically. This will put the cyberresilience on a path to re-examine its key controls and to have them accurately identified and effectively implemented. This is the optimal cyberresilience formula at any given point in time.

Achieving complete cyberthreat immunity is not possible, and even if it is attempted, it may not be worth the cost. Residual and acceptable risk (threshold) should be looked at from this perspective.

Some institutions feel that the fundamentals of cybersecurity are protecting online devices, email communication, connections, and protecting and backing up digitized information. The efforts of institutions and professionals who have recognized that cyberresilience fundamentals are centered around the protection of the enterprise assets from unauthorized access, unauthorized modification and deletion to ensure confidentiality, integrity and availability of those assets should be appreciated.

Confidentiality is guarded through internal controls that include data encryption, two-factor authentication and biometric verification. Integrity is guarded through a number of internal controls such as file access permission, cryptographic checksums and data backups. Availability is guarded through a number of internal controls that include remote facility data backups, data redundancy and firewalls.

Phase 1: Top-Down of the Model

This phase includes the hierarchical development of the enterprise assets, threats, and key controls. Steps include:

- Step 1.1: Identify critical assets of the enterprise. The critical assets are based on the fundamentals of the enterprise assets mentioned earlier data/information, people, network infrastructure and application infrastructure (**figure 2**).
- Step 1.2: Identify and list the threats for each of the identified critical assets (**figure 3**).
- Step 1.3: Identify and list key controls for the stated threats of each critical asset (**figure 4**).
- Step 1.4: Add "additional controls" in consideration of the residual risk (risk tolerance) to allow the enterprise to determine the acceptable risk threshold. In addition, it will help the enterprise quantify the required investment if and when it wants to reduce that threshold to a lower value.

Figure 3—Identified Threats

Enterprise Assets and Key Controls Cyberrisk Model				
GOAL PROTECT THE ENTERPRISE ASSETS				
CRITICAL ASSETS	**Data/Information (35 percent)**	**People (30 percent)**	**Network Infrastructure (20 percent)**	**Application Infrastructure (15 percent)**
THREATS	Data breach	Identity theft	Denial of service	Manipulation of software
	Manipulation of information	Man in the middle	Manipulation of hardware	Unauthorized installation of software
	Corruption of data	Social engineering	Botnets	Misuse of information systems
		Abuse of authorization	Network intrusion, malware	Denial of services

Figure 4—Identified Key Controls				
Enterprise Assets and Key Controls Cyberrisk Model				
GOAL PROTECT THE ENTERPRISE ASSETS				
CRITICAL ASSETS	**Data/Information (35 percent)**	**People (30 percent)**	**Network Infrastructure (20 percent)**	**Application Infrastructure (15 percent)**
THREATS	Data breach	Identity theft	Denial Of service	Manipulation of software
	Manipulation of information	Man in the middle	Manipulation of hardware	Unauthorized installation of software
	Corruption of data	Social engineering	Botnets	Misuse of information systems
		Abuse of authorization	Network intrusion, malware	Denial of services
KEY CONTROLS	Data protection (E.G., Encryption)	Controlled access	Control of privileged access	Email, web browser protection
	Data recovery capability	Account monitoring	Monitoring of Audit logs	Application software security
	Boundary defense	Security skills and training	Malware defenses	Inventory
	Additional control for residual risk	Background screening	Network controls (Configuration, ports)	Secure configuration
		Awareness of social control	Inventory	Continuous vulnerability assessment
		Additional control for residual risk	Secure configuration	Additional control for residual risk
			Continuous vulnerability assessment	
			Additional control for residual risk	

Phase 2: Quantitative Prioritization

In this phase, all attributes of the enterprise assets, threats and key controls model are prioritized (**figure 5**):

- Step 2.1: Prioritize critical assets based on importance/impact to the enterprise goal.
- Step 2.2: Prioritize the identified threats based on importance/impact on the data/information critical assets.
- Step 2.3: Prioritize the identified threats based on importance/impact on the people critical assets.
- Step 2.4: Prioritize the identified threats based on importance/impact on the network infrastructure critical assets.
- Step 2.5: Prioritize the identified threats based on importance/impact on the application infrastructure critical assets.

The preferred method of prioritization for a hierarchical model is the analytic hierarchy process (AHP). AHP is an excellent technique for prioritization.

Figure 5—Quantitative Prioritization of Critical Assets, Threats and Key Controls

Enterprise Assets and Key Controls Cyberrisk Model				
GOAL PROTECT THE ENTERPRISE ASSETS				
CRITICAL ASSETS	**Data/Information (35 percent)**	**People (30 percent)**	**Network Infrastructure (20 percent)**	**Application Infrastructure (15 percent)**
THREATS	Data breach (40%)	Identity theft (20%)	Denial of service (18%)	Manipulation of software (24%)
	Manipulation of information (35%)	Man in the middle (15%)	Manipulation of hardware (12%)	Unauthorized installation of software (20%)
	Corruption of data (25%)	Social engineering (40%)	Botnets (10%)	Misuse of information systems (14%)
		Abuse of authorization (25%)	Network intrusion, malware (60%)	Denial of services (42%)
KEY CONTROLS	Data protection (E.G., Encryption)	Controlled access	Control of privileged access	Email, web browser protection
	Data recovery capability	Account monitoring	Monitoring of Audit logs	Application software security
	Boundary defense	Security skills and training	Malware defenses	Inventory
	Additional control for residual risk	Background screening	Network controls (Configuration, ports)	Secure configuration
		Awareness of social control	Inventory	Continuous vulnerability assessment
		Additional control for residual risk	Secure configuration	Additional control for residual risk
			Continuous vulnerability assessment	
			Additional control for residual risk	

The cyberrisk model is most credible when it is developed with participation from the key enterprise stakeholders representing various functional entities. It is conducted through workshop sessions led by a facilitator using the AHP technique to determine the degree of quantifiable impacts/priorities of each element in the hierarchical cyberrisk model.

The unique aspect of AHP is that the enterprise stakeholders can build their own cyberrisk model with specific elements and priorities they see fit for their organization at the time.[9]

AHP: Pairwise Comparison and Establishing Priorities

AHP starts by refining a complex problem into smaller elements. It then organizes the elements into sets of homogeneous clusters, which are subdivided into more detailed sets until the lower levels of the hierarchy are established. This structure represents the total view of the model (e.g., enterprise) being studied.

AHP helps its users deal with complex problems (e.g., cybersecurity initiatives justifications) by representing the enterprise in hierarchical form and identifying the major elements within each level, depending on the level of detail required.

The number and type of elements within each level in the hierarchy depend on the enterprise's business environment.

AHP compares any two elements in a given layer and measure the degree of impact on any element in the layer above it. The pairwise comparisons are repeated with every element in each level, starting from the top level and continuing downward to the lowest level of the decision model hierarchy.

AHP helps establish priorities by asking the workshop participants to state the degree of impact of the pairwise comparisons of the element sets in each level in the hierarchy structure with respect to each of the elements in the next higher level.

Phase 3: Bottom-Up of The Model

The illustration of this phase and its steps are depicted in **figures 6 through 9**:

- Step 3.1: Classify each type of critical asset into different tiers. For the purposes of this discussion, three-tier classifications are used.
- Step. 3.2: Prioritize the identified key controls to each of the identified threats listed under the fundamental assets based on the classification of the identified critical assets, such as tier 1, tier 2 and tier 3. This is a reflection of the assets' importance/impact and in consideration of the magnitude of the identified threats associated with the asset type.
- Step 3.2.1: For example, critical assets related to data/information could be classified in the following tiers:
  - **Tier 1: Confidential**—Assets related to financial information, secret formula, PII or protected health information (PHI)
  - **Tier 2: On a Need to Know**—Data for internal use only, customer information, HR policies, employee list
  - **Tier 3: Available to Public**—The lowest level of classification in which disclosure will not cause serious negative consequences to the enterprise, website content or other open-source information
- Step 3.2.2: For example, classify role-based access control (RBAC) related to people in the following tiers:
  - **Tier 1: Very High Privileged Users**—Super systems administrator

Figure 6—Prioritized Key Controls to the Tier: "Data/Information" Asset Type, Based on Threat "Data Breach"

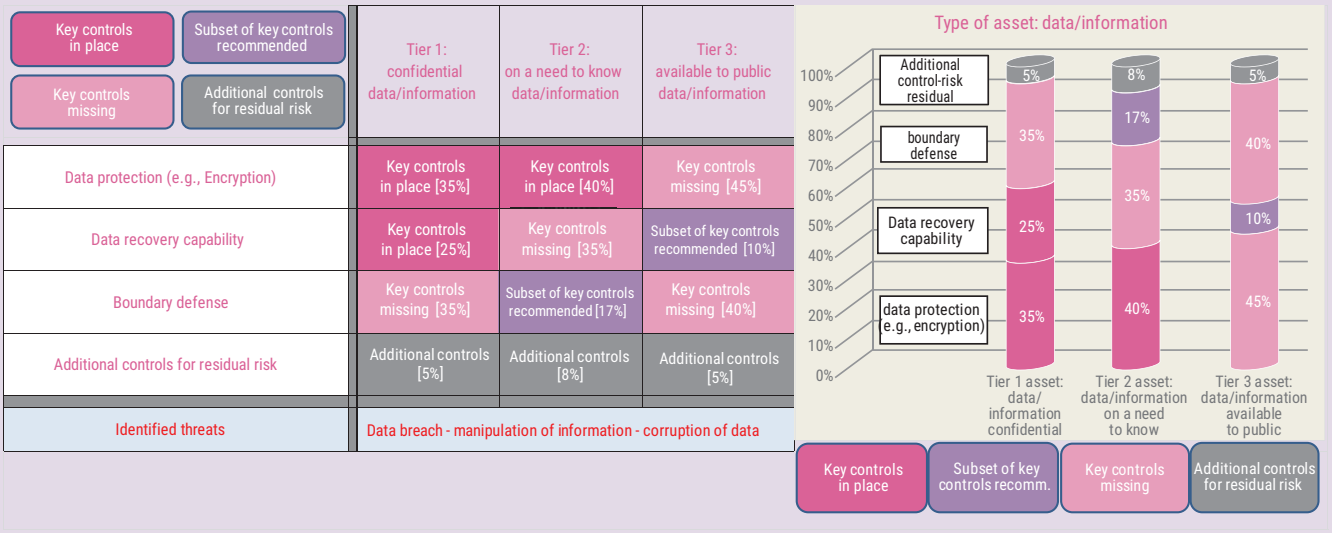


Figure 7—Prioritized Key Controls to the Tier: "People" Asset Type, Based on Threat "Social Engineering"

Type of asset: people	Tier 1: very high privileged users [People]	Tier 2: super users [People]	Tier 3: standard user [People]
Controlled access	Key controls In place [35%]	Key controls In place [35%]	Key controls missing [25%]
Account monitoring	Key controls In place [20%]	Key controls missing [15%]	Subset of key controls recommended [20%]
Security skills and training	Key controls missing [15%]	Subset of key controls recommended [15%]	Key controls missing [20%]
Background screening	Subset of key controls recommended [20%]	Subset of key controls recommended [15%]	Key controls missing [15%]
Awareness and social control	Key controls missing [7%]	Subset of key controls recommended [13%]	Key controls missing [16%]
Additional controls for residual risk	Additional controls [3%]	Additional controls [7%]	Additional controls [4%]
Identified threats	Identity theft - man in the middle - social engineering - Abuse authorization		

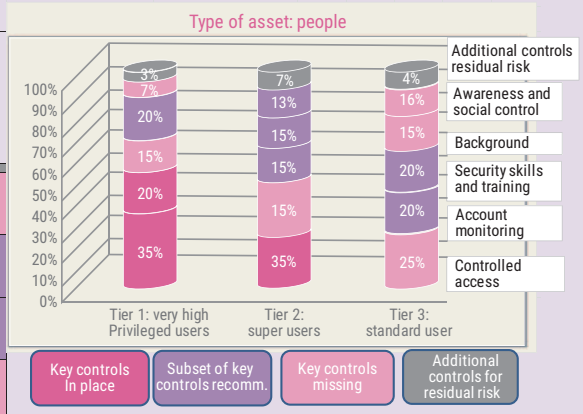
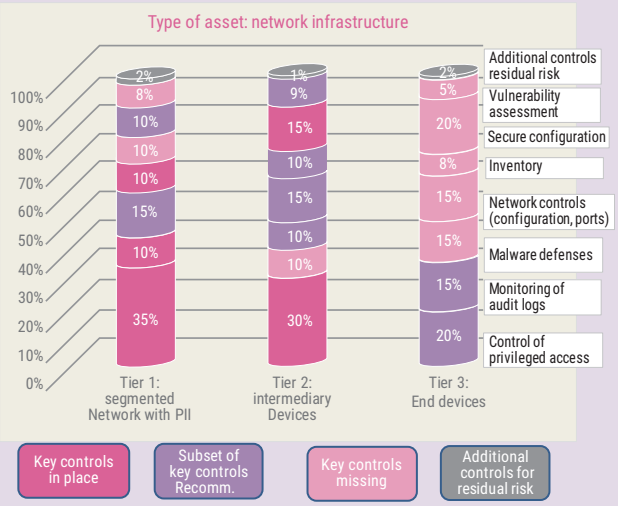


Figure 8—Prioritized Key Controls to the Tier: "Network Infrastructure" Asset Type, Based on Threats "Network Intrusion and Malware"

Type of asset: network infrastructure	Tier 1: segmented network with PII [network infrastructure]	Tier 2: intermediary devices [network infrastructure]	Tier 3: end devices [network infrastructure]
Control of privileged access	Key controls in place [35%]	Key controls in place [30%]	Subset of key controls recommended [20%]
Monitoring of audit logs	Key controls in place [10%]	Key controls missing [10%]	Subset of key controls recommended [15%]
Malware defenses	Subset of key controls recommended [15%]	Subset of key controls recommended [10%]	Key controls missing [15%]
Network controls (configuration, ports)	Key controls in place [10%]	Subset of key controls recommended [15%]	Key controls missing [15%]
Inventory	Key controls missing [10%]	Subset of key controls recommended [10%]	Key controls missing [8%]
Secure configuration	Subset of key controls recommended [10%]	Key controls in place [15%]	Key controls missing [20%]
Continuous vulnerability assessment	Key controls missing [8%]	Subset of key controls recommended [9%]	Key controls missing [5%]
Additional controls for residual risk	Additional controls [2%]	Additional controls [1%]	Additional controls [2%]
Identified threats	Denial of service - manipulation of hardware - botnets - Network intrusion/malware		

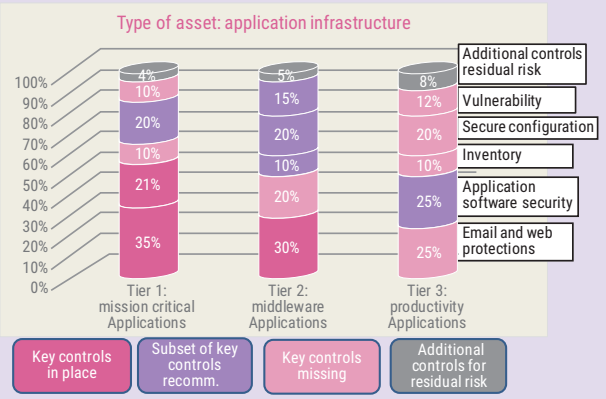


- **Tier 2: Super Users**—Systems administrator, user with highly privileged accounts
- **Tier 3: Standard Users**—Regular employee with limited or restricted administrative access

- Step 3.2.3: For example, classify critical assets related to network infrastructure in the following tiers:
  - **Tier 1: Segmented Network with PII Information**—Network access to servers contains credit card users and numbers

Figure 9—Prioritized Key Controls to the Tier: "Application Infrastructure" Asset Type, Based on Threat "Denial of Service"

Type of asset: application infrastructure	Tier 1: mission critical applications [application infrastructure]	Tier 2: middleware applications [application infrastructure]	Tier 3: productivity applications [application infrastructure]
Email and web browser protections	Key controls In place [35%]	Key controls In place [30%]	Key controls missing [25%]
Application software security	Key controls In place [21%]	Key controls missing [20%]	Subset of key controls recommended [25%]
Inventory	Key controls missing [10%]	Subset of key controls recommended [10%]	Key controls missing [10%]
Secure configuration	Subset of key controls recommended [20%]	Subset of key controls recommended [20%]	Key controls missing [20%]
Continuous vulnerability assessment	Key controls missing [10%]	Subset of key controls recommended [15%]	Key controls missing [12%]
Additional controls for residual risk	Additional controls [4%]	Additional controls [5%]	Additional controls [8%]
Identified threats	Manipulation of software - unauthorized installation of software - misuse of information systems - denial of service		



  - **Tier 2: Intermediary Devices**—Switches and wireless access point (network access) routers (Internetworking)
  - **Tier 3: End Devices**—Computers (workstations, laptops, web servers), mobile devices, iPad, Internet of things (IoT)
- Step 3.2.4: For example, classify critical assets related to application infrastructure in the following tiers:
  - **Tier 1: Mission Critical Applications**—Email, accounting, production and supply chain applications
  - **Tier 2: Middleware Applications**—Application development tools, application programming interface (API), remote procedure call (RPC)
  - **Tier 3: Productivity Applications**—Office productivity applications, desktop publishing, Microsoft Office

If there are many key controls (e.g., more than six), the prioritization/impact will be highly diluted when reporting to the BoD and executive teams. However, there will be other subcontrols within each key control. The decision and degree of implementation must be left up to the stakeholders and cyberresilience team.

Advantage of the Illustrated Cyberrisk Model

The current gaps between the enterprise BoD, senior executives and cyberprofessionals who are diverse in culture and background include a lack of accurately presenting risk, threats and remediation in the right context. Explanations and understandings of risk have different meanings to the BoD and cyberprofessionals. Bringing BoDs and cyberprofessionals to a common platform is vital to the enterprise. The proposed cyberrisk model ensures among the stakeholders a common and communicated understanding of:

- What are the enterprise priorities
- What assets require protection
- What type of threats are looming
- What key controls should be in place
- What residual risk the enterprise can tolerate

Because cyberrisk containment is the responsibility of all enterprise stakeholders and they should be held accountable, a holistic approach and methodology that enables the facilitation and communication of such encompassing accountability is needed. The end product of the

> "EXPLANATIONS AND UNDERSTANDINGS OF RISK HAVE DIFFERENT MEANINGS TO THE BOD AND CYBERPROFESSIONALS."

cyberrisk model is the translation of the enterprise priorities to the cyberprofessionals. In turn, cyberprofessionals translate such directives into actionable key controls to implement, manage, monitor and report. The final result achieved is an effective management of risk, an accurate cyberbudget and greater resource utilization.

Qualitative benefits of the enterprise assets and key controls cyberrisk model include:

- Alignment of cybergovernance to the enterprise priorities
- Focus on cyberrisk, threats and essential key controls for various assets
- Focus on economic investments, resource allocation and priority of initiatives
- Removal of complexity and confusion by clarifying cyberstrategy
- Establishment of clear communication with various stakeholders: executive team, senior management and technical staff
- Enablement of effective monitoring and meaningful cyberreporting
- Permission to revisit and recalibrate enterprise posture when assets, threats and technology are changing
- Formation of an effective cyber organization with clear job requirements and responsibilities
- Transitioning the enterprise from cybersecurity to cyberresilience culture
- Improvement of cyber processes, policies and procedures

Using consensus and prioritization methods to apply the AHP technique in the enterprise model, completing workshop sessions managed by facilitators and ensuring diversity of stakeholders representing various enterprise functions will ensure the objectivity, accuracy and management support needed for the quantifiable conclusions and recommendations of the enterprise assets and key controls cyberrisk model.

Endnotes

1 Lietz, C.; N. Son; *Cybersecurity and The Board of Directors: Tips for Securing Support for Your Cyber Risk Management,* Coalfire Systems, Inc., USA, 2016, *https://www.coalfire.com/documents/whitepapers/coalfire_wp_bod.pdf*

2 Osterman Research, Inc., *Reporting to the Board: Where CISOs and the Board Are Missing the Mark*, USA, February 2016, *https://www.american.edu/kogod/research/cybergov/articles/upload/article-of-march-2016_reporting-to-the-board.pdf*

3 *Ibid.*

4 Putrus, R.; "Enterprise Transformation to Cyberresiliency," *ISACA® Journal*, vol. 3, 2019, *https://www.isaca.org/archives*

5 *Ibid.*

6 Chan, D.; J. Kaplan; A. Weinburg; "Risk and Responsibility in a Hyperconnected World: Implications for Enterprises," McKinsey & Company, January 2014, *https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/risk-and-responsibility-in-a-hyperconnected-world-implications-for-enterprises*

7 Poppensieker, T.; R. Riemenschnitter; "A New Posture for Cybersecurity in a Networked World," McKinsey & Company, 9 March 2018, *https://www.mckinsey.com/business-functions/risk/our-insights/a-new-posture-for-cybersecurity-in-a-networked-world*

8 *Ibid.*

9 Saaty, T. L.; *Decision Making for Leaders: The Analytic Hierarchy Process for Decisions in a Complex World,* Lifetime Learning Publications, USA, 1982