SECURITY

A RISK-AWARE PATH TO CYBERSECURITY RESILIENCE AND MATURITY

CMMI® Institute

ISACA®

CONTENTS

ABSTRACT

Cybersecurity is approached, analyzed and managed usually from a functional point of view, but measuring security coverage and utility is not enough anymore. Cybersecurity is not about a series of tasks. The challenges of cybersecurity are huge and increasingly complex. Cybersecurity must consider business strategy planning and performance as capability. Analyzing the capability of cybersecurity within an enterprise means systematically and holistically analyzing the operational efficiency of actions taken, resiliency of the people/processes/technology in use, maturity of practices, gap analyses, total cost of ownership, and more, together with effectiveness, and doing it comprehensively and consistently across the axis of risk. Looking at cybersecurity in this way requires a new mindset and new tools. Fortunately, methods already exist that can be harnessed to assess cybersecurity. This white paper outlines the practical cybersecurity challenges in enterprises—challenges that are already acute and increase organizational and business risk, because capability gaps are not recognized, prioritized and resolved. Read this white paper to discover how to adapt your enterprise to a cybersecurity capability mindset and understand its importance on instilling a culture of cybersecurity throughout your enterprise and board of directors.

A Risk-Aware Path to Cybersecurity Resilience and Maturity

Cybersecurity is typically approached, analyzed and managed from a functional point of view. Enterprises typically spend considerable and growing amounts of time and resources analyzing their security programs—and by extension the countermeasures comprising them—through the lens of scope and function. Cybersecurity teams look at whether individual countermeasures (e.g., controls) function appropriately, their coverage is sufficient to close risk gaps and they are implemented appropriately. The most common security performance measures available to enterprises (e.g., vulnerability assessment, penetration testing and risk assessments) measure exactly those points—coverage and utility.

But measuring coverage and utility is not enough anymore and has not been enough for some time.

These approaches to cybersecurity—program, management and measurement—are increasingly inadequate to the task, because cybersecurity is not about a series of tasks. The challenges of cybersecurity are huge and increasingly complex, whether the context is business ecosystems, government agencies, healthcare systems, critical infrastructure or others. Clearly, there is more to security measurement beyond coverage and utility. Cybersecurity must consider business strategy planning and performance as capability. Analyzing the capability of cybersecurity within an enterprise means systematically and holistically analyzing the operational efficiency of actions taken, resiliency of the people/processes/technology in use, maturity of practices, gap analyses, and total cost of ownership, and more, together with effectiveness, and doing it comprehensively and consistently across the axis of risk. For example, analyzing the capability of cybersecurity can be done by evaluating what specific controls and countermeasures offset the most risk, based on the specific risk that the enterprise, or a portion of the entity, might encounter, given its mission, the operating environment and the type of attacks that it might encounter.

Looking at cybersecurity in this way requires a new mindset and new tools. Fortunately, methods already exist–cultivated over decades and millions of dollars of investment–that can be harnessed to assess cybersecurity capability in this fashion. This white paper outlines the practical challenges of cybersecurity in enterprises—challenges that are already acute and only increase organizational and business risk because capability gaps (i.e., areas where a capability does not exist) are not recognized, prioritized and resolved. Further, this white paper describes how to adapt to a capability mindset and its importance on instilling a culture of cybersecurity, from the frontlines to board seats.

A Mindset Reset

Most executives are accustomed to asking themselves the question, “Is my enterprise secure?”, or, for regulated enterprises, “Am I compliant?” Most cybersecurity practitioners are probably accustomed to providing information to help answer those questions.

A question that practitioners and executives might be less accustomed to asking is, “Is our security program operating effectively?” Note that this question is a more nuanced question than “Am I compliant?” or “Am I secure?” Asking whether the security program is effective goes a step further than evaluating whether an enterprise’s security program (and by extension the controls/countermeasures employed to support that program) keeps bad guys out, malware from spreading or enforces specific policy. This question means a few other things as well.

Specifically, the question “Is our security program operating effectively?” asks whether the security program is tailored appropriately for the risk that the enterprise will encounter. This is driven by the type of business, the environment in which the enterprise operates, its organizational risk tolerances, organizational culture and any number of other (sometimes enterprise-specific) factors. The question also asks whether processes and mechanisms supporting security goals are mature—resilient against employee attrition, reductions in budget or emergency situations. It asks whether security countermeasures are resource optimized. It is a much bigger question.

Ascertaining if an enterprise’s security operates effectively means looking at cybersecurity through the lens of capability. How optimized, effective, resilient and mature is the way that security is delivered? Just as a physical lens filters and focuses light energy, the lens of capability filters and focuses understanding of risk. It filters it so that enterprises ensure that measures taken are optimized—that the most risk is reduced in the most cost-effective way possible (allowing reinvestment of budget into risk mitigation somewhere else). Likewise, the lens of capability focuses that risk information (incorporating information already in place, such as risk assessments and other measurement instruments) to build in the right level of maturity and resiliency for those measures that are most critical. However, the relationship between maturity and resiliency is not one of equals. A resilient enterprise is one that has achieved the necessary risk-based maturity for capabilities that address enterprise risk. Therefore, maturing capabilities are the path to building resiliency. While maturity does not automatically ensure resilience, maturity is a necessary component for resilient security measures and a key ingredient in ensuring reliable, consistent outcomes.

There are a few reasons why it is advantageous for enterprises to embrace this mindset. It is a given that enterprises need to address cybersecurity. Ideally, they do so holistically; barring that, they at least implement individual countermeasures to address specific technical risk, operational risk or compliance requirements. But it behooves enterprises to go beyond this—to manage how they do it and whether they do it. Asking how they do it is a principle of good governance; it means they get the most value from the work they do, they fully leverage investments, they use resources optimally, and they make informed, risk-aware decisions.

Today's Cybersecurity Reality

This document provides a call to action and supporting guidance to highlight how and why employing a capability-aware perspective is advantageous to individual enterprises today and an optimal path forward for the profession. However, understanding why this is the case must start with understanding the current state of cybersecurity for most enterprises, including a frank discussion of existing challenges. By understanding how and why the current challenges exist, the advantages of a capability-aware understanding become more apparent and more compelling.

Cybersecurity practitioners—and by extension, the enterprises they serve—face many challenge areas, including:

- Risk management
- Due diligence and negligence
- Operational efficacy and efficiency
- Prioritization
- Security operations
- Skill sets and training
- Budget—responsibility and accountability.

To understand them thoroughly, each area requires more detailed discussion, which is provided in the following sections.

Risk Management

Enterprises struggle with risk management—they either are not doing it, do it poorly or think they are doing it when they are not. This is true even in enterprises that have a regulatory mandate to address risk management.

To see this in action, look at the track record for healthcare entities in the United States that currently have a regulatory mandate to address the US Health Insurance Portability and Accountability Act (HIPAA). These entities have had, for the past 20 years, a regulatory requirement to undertake risk management. Specifically, HIPAA requires enterprises to assess risk[1] and manage that risk.[2] In September 2017, the US Department of Health and Human Services (HHS) Office for Civil Rights (OCR), the regulatory entity responsible for HIPAA enforcement, published the initial results of the findings to date, from a 2017 audit of covered entities.[3] One of the most problematic areas was risk management.

Of the 63 covered entities that the OCR examined, 17 (27 percent) were given the lowest possible rating, indicating that, "The entity did not provide OCR with evidence of [a] serious attempt to comply with the Rules and enable individual rights with regard to PHI."[4] A further 63 percent were given the second-lowest rating, indicating that, "…the entity made negligible efforts to comply…" Meaning, the risk management value, for 90 percent of the covered entities, was either "negligible" or "none."[5]

[1] HIPAA Security Rule required implementation specification §164.308(a)(1)(ii)(A): "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity." For more information: U.S. Department of Health & Human Services, Guidance on Risk Analysis, HHS.gov, *www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html*

[2] HIPAA Security Rule required implementation specification §164.308(a)(1)(ii)(B): "Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a)." For more information: U.S. Department of Health & Human Services, Guidance on Risk Analysis, HHS.gov, *www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html*

[3] Sanches, Linda; "Update on Audits of Entity Compliance with the HIPAA Rules," September 2017, *www.nist.gov/sites/default/files/documents////sanches_0.pdf*

[4] *Ibid.*

[5] *Ibid.*

While this is one data point from one sector of industry, it should serve to illustrate the point that risk management is not executed ubiquitously or effectively in enterprises. There are a few reasons why this is true. First, risk tolerances are often difficult to obtain, and, even after they are obtained, can be a moving target. For example, a risk might have one priority when it is theoretical and another priority when it is actively faced by the enterprise. An analogy is flood insurance: someone might perceive that to take a chance that it will not flood and forego the insurance is more acceptable when it has never flooded, compared with their perception right before a hurricane is scheduled to hit.

Another reason why risk management is not executed ubiquitously or effectively in enterprises is that there can often be a disconnect between risk that an enterprise faces and the specific countermeasures and practices that are driven by regulatory compliance. A situation can arise forcing those in the enterprise to decide if they implement one control, because it addresses a regulatory or customer requirement, or a different control that has (for them) more overall risk reduction. One can argue that risk reduction is overall a better use of enterprise resources, but meeting the requirements of a regulation is often nonoptional.

Compliance-driven efforts, while ensuring that a minimum baseline is met, sometimes do so without accounting for the specific risk that the enterprise might encounter. These efforts are in many cases noncustomizable, meaning that every enterprise under the umbrella of that regulation must meet the same level of compliance. Although, for some enterprises, this minimum baseline may be sufficient for risk mitigation and compliance, for many enterprises, it will not. Likewise, compliance-driven efforts may be compartmentalized in scope. For example, the Payment Card Industry Data Security Standard (PCI DSS) applies only to areas that store, process or transmit credit card information; HIPAA applies only when protected health information (PHI) is impacted. True risk management is holistic rather than compartmental in scope and, thereby, extends beyond merely complying with a mandated minimum level.

Lastly, enterprises are becoming increasingly complex. Risk management requires that enterprises understand a few things that are hard to quantify or qualify, e.g., the likelihood of a situation occurring; the impact should it do so; the relative difference in likelihood or impact, before vs. after a countermeasure is applied. Each one of these points is supported by so many independent variables, influenced by many “what if” scenarios, and contains so many outliers and unique situations that it is not hyperbole to say that an enterprise could invest its entire security budget in risk management and it may still not be 100-percent perfect.

Due Diligence and Negligence

The second challenge area has to do with ensuring appropriate due diligence. Security practitioners say that due diligence is critical—meaning it is a legal imperative (and many practitioners would argue a moral and ethical one also) into which enterprises invest time, energy and budget, making sure they take appropriate measures (based on industry-accepted norms and standard of care) to address security. It is a given that addressing security is important. What is not a given is specifically what these measures are. What is appropriate and reasonable? What are the norms? What is the standard of care?

As a practical matter, appropriate measures to address security can often be hard to determine. Enterprises are often (rightly) secretive about their security controls and even specific goals. Although this opacity about security is reflective of normative practice, the effect is that it is challenging for one enterprise to use experiences from another enterprise as a guidepost. Any given enterprise might have a rough outline of accepted practice based on guidance (e.g., standards and frameworks), but these can differ from industry to industry, based on geography or based on intended audience. Likewise, regulatory mandates provide a guidepost, but as noted previously, they define a minimum baseline rather than a complete taxonomy of industry norms and practice.

The situation is further compounded, though, because standard of care may not always align with industry culture and norms. The easiest way to understand this is through the often-cited T.J. Hooper decision.[6] In this case, the operators of the T.J. Hooper (a tugboat that, in 1928, sank with several barges in tow[7]) were sued for negligence, because a radio (not installed on the tugboat) would have prevented the T.J. Hooper from sinking if the radio had been installed. The judge in this case concluded that, despite maritime radio use not being generally accepted practice, it was nevertheless the responsibility of the T.J. Hooper's owners to install one. The judge decided that the safety value provided by the radio, relative to the cost, made it negligent to fail to install one. This in turn means that risk, not standard practice or industry norms, determines whether an action is negligent.

While the T.J. Hooper decision focused on the presence of technology, it is important to remember that today's risk environment focuses not only on technology, but those responsible for using it. Given that threats are pervasive, a hardened IT and cybersecurity workforce is critical. Enterprises must, to the greatest extent possible or practical, institutionalize the knowledge necessary to address risk. Although technologies tend to become the focus when discussing vulnerabilities, it is imperative to remember that professionals also present their own potential as sources of vulnerability, and steps must be taken to mitigate that.

Operational Efficacy and Efficiency

Two (sometimes competing) interests—efficacy and efficiency of security measures—are at work for security teams that, to be measured and assessed, typically need to be analyzed separately.

Efficacy relates to whether security measures are sufficient and whether they are working as intended. Generally, when an enterprise assesses its security efforts, it looks in detail at efficacy of what the security program is doing or the operation of a specific control. For example, a third-party audit review, such as one initiated by a customer or a regulator, typically examines efficacy in detail. Likewise, a first-party audit or self-assessment examines this. To analyze efficacy, one must evaluate whether controls in place are sufficient, in line with risk, informed by the threat environment, performing as expected, and so forth.

For an enterprise to fully optimize the security program, it must include another dimension in addition to efficacy—namely, it must also assess efficiency. An example compares two potential antimalware controls. The first is scanning software that compares individual files against a database of known malware (how most antimalware software operates). The second is a consultant who is paid to manually review files with a hex editor. These two approaches perform an equivalent function (find and alert the security team to the presence of malware.) Even in the unlikely event that they perform the task with identical accuracy, they have very different operational characteristics. The time required to analyze is different, the resiliency of the process to

[6] 4LawSchool.com; "The T.J. Hooper Case Study," 60 F.2d 737, *http://www.4lawschool.com/torts/hooper.shtml*

[7] ISACA; "Is the TJ Hooper Case Relevant for Today's Information Security Environment?," ISACA Journal, 2013, *https://www.isaca.org/Journal/archives/2013/Volume-2/Pages/Is-the-TJ-Hooper-Case-Relevant-for-Todays-Information-Security-Environment.aspx*

employee attrition is different, potential for human error is different and the value returned for the money invested is different. In most circumstances, one approach is a vastly better business decision than the other.

Although this is clearly an exceptional example (i.e., a simplistic one and with deliberately hyperbolic operational requirements to illustrate the dichotomy), it is by no means an unusual or entirely unheard-of tradeoff in other areas. Decisions about how to approach specific controls are made daily. One enterprise may implement a log correlation tool, while another enterprise reviews logs manually. Some enterprises may build a threat analysis team internally, while others subscribe to a feed. For any given security outcome, a near-infinite array of choices exists for how to achieve it. Guidance on how to optimize these aspects of operation has been much less forthcoming than guidance about achieving specific security outcomes.

Prioritization

On the surface, the prioritization of which countermeasures to implement might sound like a direct risk management exercise, i.e., one invests in deploying the controls that provide the most risk reduction value. However, in practice, there are a few reasons why it can be significantly more complicated than this.

First, the increasing array of regulatory mandates, frameworks and guidance documents that are germane to any given enterprise can complicate prioritization. In the best cases, specific controls within them overlap such that, by addressing one, multiple different requirements are addressed across the full list. But, this only happens some of the time. Because each of these guidance documents has its own context, it also has its own expectations. Therefore, as a practical matter, individual measures can vary greatly. In some cases, they can be contradictory.

Additionally, some implementation steps can address parts of multiple goals, such as, when the implementation of a risk mitigation measure is easier, if another task is undertaken first. For example, consider two controls—cloud configuration management and asset discovery/inventory (part of asset management). These controls are useful measures on their own and provide risk reduction value. For many enterprises, cloud configuration management might provide more risk reduction potential overall, than technology discovery. However, implementing configuration management is significantly more challenging when the inventory does not exist. In this case, resources might be best used by pursuing the implementation of these controls in other-than-risk-offset order.

Security Operations

The mechanics of security operations are another challenge area for enterprises. Obtaining adequate funding and shortage of appropriate skills can create challenges. For example, the 2016 E&Y Global Information Security Survey revealed that 61 percent of executives cited budget constraints as one of their primary challenges, and 69 percent said they would need up to an additional 50 percent of budget to operate effectively.[8] Regarding skills, 55 percent of the ISACA 2017 Global State of Cybersecurity Survey respondents indicated open security positions take three months or longer to fill; one quarter of them responded that positions can take as long as six months to find a qualified candidate.[9]

These challenges create pressure on operations teams. As a practical matter, they are underfunded, while staffing challenges create additional pressures. These

[8] Ernst & Young Global Limited; "Path to cyber resilience: Sense, resist, react: EY's 19th Global Information Security Survey 2016-17," EY, 2017, *http://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2016*

[9] ISACA; "State of Cyber Security," 2017, *https://cybersecurity.isaca.org/state-of-cybersecurity*

two situations feed off each other—lack of personnel available to operate a tool or other technology can lead to lost value from investments already made, while lack of budget to acquire technology can lead to inefficiencies in staff time. Therefore, processes that are heavily reliant on human expertise are less resilient—staff attrition can result in suboptimal performance of countermeasures or otherwise prove detrimental to existing processes.

Underfunding and staffing challenges are among the chief challenges facing security operations, but they are by no means the only ones. Mission priorities can manifest themselves in difficulties for security operations to surmount, as can available or even legacy technologies. For example, an enterprise may need to make a decision about how to use resources strategically. One priority may be to secure existing assets, and another competing challenge may be to capitalize on areas of opportunity in ways that are more directly business- or enterprise-visible. Security investments, although necessary, are seldom as compelling as opportunities that directly increase revenue or that otherwise directly forward a business goal.

Even if those internal challenges are met, there is also the external threat landscape to consider. Attackers and defenders are in an ever-advancing arms race—attackers develop increasingly sophisticated tradecraft while defenders improve defense techniques. The threat landscape constantly shifts as new attack methods are developed. The threat landscape is asymmetric, because defenders are required to mitigate every possible avenue of attack, but attackers need find only one pathway to get in.

Withstanding Tomorrow’s Threats

Cybersecurity has few, if any, one-size-fits-all solutions. Each enterprise is unique, as are its needs and goals. The major challenge areas that are discussed in the previous sections (risk management, due diligence and negligence, operational efficacy and efficiency, security operations, and prioritization) impact every enterprise, but the ways they impact them are as unique to each enterprise as a fingerprint.

However, even fingerprints share commonalities; enterprises are no different. Prioritizing within risk management efforts and determining how the enterprise’s ability to deliver on security goals (and the cost to implement that) compares to others within its industry remain universally challenging. Likewise, the disparate elements of security, risk management and infrastructure resilience must continue to function securely; each element of an overall security approach must continue to operate effectively to prevent against different threats and risk scenarios. Individual components and elements must continue to operate effectively and reliably, despite the addition of new controls or countermeasures, and in the presence of change.

When solving the cybersecurity problems besetting an enterprise, what will be done and how it will be done must be determined. Enterprises need to answer the following questions:

- Is our enterprise optimizing its available resources as it satisfies the problem?
- Are we situationally aware/clear?
- Are we asking the right questions about risk and using the responses to those questions to inform our decisions?
- Are we exercising strong governance to ensure our enterprise obtains return on investment not only on the investments in resources it makes, but on the work that is performed?

Most importantly though, these questions must be asked across the dimension of time. Cyberthreats to an enterprise do not operate on a 9-to-5, major-holidays-observed basis. Enterprises are just as likely to be tested by a cyberattack on a June Tuesday at 10 a.m. as at 1 a.m. on Boxing Day. It is for this reason that, ultimately, cybersecurity must be viewed as a core functional capability of an enterprise at any time, day-in, day-out, 24/7/365, and as a strategic business imperative.

Doing all these things requires viewing the discipline of security as a capability—a holistic strategy and the supporting elements within it, which are optimized to the extent practicable, resilient against attack and operating as intended, despite interference or change to the enterprise.

Organic Standard

To examine mechanisms for how to practically answer the above questions in an ongoing way, one must start by examining how most enterprises approach security generally. As previously noted, for many enterprises, the starting point is compliance, specifically, evaluating themselves against a list of required or desired controls or countermeasures (i.e., security tools and practices). These tools and practices originate from regulatory mandates, best practice frameworks (e.g., the ISACA COBIT 5 management practices) or other security standards (e.g., ISO 27001). These standards, frameworks and guidance are used either indirectly—as input into risk management activities— or directly—as a benchmark against which they evaluate their program and the specific methods they employ.

Looking at cybersecurity in this way is problematic for a few reasons. For one, these standards are written at a point in time, from a particular point of view and for a particular audience. For example, HIPAA was authored in 1996; the most recent provisions (the omnibus rule) were published by HHS in March 2013.[10] These regulations are purposefully released slowly to allow the broadest segment of industry to comply. The risk landscape seldom changes with this slow of a cadence.

These measures also sometimes codify measures that are unnecessary or that introduce other burdens. For example, NIST recently (the summer of 2016) updated password guidance in the draft revision of *SP800-63-3: Digital Authentication Guidelines*.[11] This update revisits past guidance about password complexity—rules and traditional wisdom about password characteristics that have been accepted for decades. Were prior measures that were challenging for users to adhere to and for enterprises to mandate even necessary? The research, while not definitive, suggests perhaps not (as reflected in the new guidance.)

Although these standards are useful in building a capability-aware cybersecurity approach, new organic standards must be able to adapt and evolve based on changes in technology, risk, attacker behavior or any number of other factors.

Perhaps the best analogy for organic standards can be found in the living nature of statutory law. As case law is made, and legislative measures are passed that amend, remove or add to existing statutory frameworks, the law itself evolves to recognize and incorporate these changes. This type of dynamism—controlled, gradual and continual evolution within a preexisting framework—is well-suited to cybersecurity. The threat landscape evolves continually—new threat actors emerge, their interests and areas of focus shift, and their tradecraft evolves and becomes more sophisticated. Likewise, the specific vulnerabilities these threat actors employ constantly evolve; new vulnerabilities arise near-constantly while old ones are being fixed and addressed. These developments occur in parallel with changes to enterprises and the technology they employ.

[10] U.S. Department of Health & Human Services; "HIPAA Administrative Simplification, Regulation Text, 45 CFR Parts 160, 162, and 164," March 2013, *https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf*

[11] Grassi, Paul A.; Michael E. Garcia; James L. Fenton; "Digital Identity Guidelines, NIST Special Publication 800-63-3," June 2017, *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf*

This, in turn, means that any regulation, industry consensus, guidance, framework or other artifact put in place is quickly, upon release, overcome by events if it cannot adapt. To combat this outcome, there must be ways for the industry to measure the cybersecurity capability and resilience of an enterprise that can adapt and still maintain relevance. Traditional standards, technical or otherwise, are not built to be future-proof and to evolve. Although they are effective, valuable and ultimately beneficial in many respects, they lack the capacity to evolve rapidly and, in a highly dynamic environment, may not the best tool for the task of optimally addressing risk.

Organic standards, by contrast, can and should incorporate developments and changes within the threat landscape. To the extent that it is possible to build such a standard, it would become more relevant as time passes, rather than less relevant. An organic standard can adapt with the threat landscape; it can likewise adjust with an enterprise's risk posture—as an enterprise adapts how it functions, that which is identified as risky potentially changes.

Objective Benchmarks

More than two millennia ago, the Chinese military strategist Sun Tzu wrote:

> *If you know your enemies and know yourself, you will not be imperiled in a hundred battles. If you do not know your enemies, but know yourself, you will win one battle for every battle you lose. If you do not know your enemies nor yourself, you will be imperiled in every single battle.*[12]

This quote goes to the heart of cybersecurity capability. An enterprise's internal focus (know yourself) provides it with the knowledge of what it can and cannot accomplish, but that focus remains only one side of the equation. An external focus (know your enemies) must have equal relevance. This external focus, however, cannot be solely confined to the threat landscape. It must also include an objective analysis of where an enterprise stands among those enterprises it wishes to measure itself against.

When enterprises engage in this sort of analysis, it enables the enhanced generation of cybersecurity capabilities and maturity. The external focus provides enterprises with the ability to measure their actions against what others within their cohort are doing to provide cybersecurity protection for their respective enterprises. The external focus also enables enterprises to establish more-defensible due-care standards for themselves (i.e., to allow them to demonstrate that reasonable protection measures are in place), because this focus provides the enterprise with a better view of the landscape and the impact its actions or inactions can have on another enterprise.

Knowing how an enterprise compares with others enables improved baselining of its highest performing cybersecurity resources, because now it is comparing how its resources perform to similar enterprises using the same resources, for many of the same reasons. The knowledge that comes from objective comparisons gives enterprises a deeper understanding of where they are in cybersecurity capability and maturity, whether that is defined as within an industry or market sector, within the boundaries of a geographic region, or in comparison to other enterprises of similar size or type. Knowing how an enterprise compares to other enterprises in cybersecurity capability and maturity is also crucial to the cycle of continuous improvement that enterprises must maintain, because this knowledge provides a broader comparison of how returns on resource investments are faring in other comparative enterprises.

[12] Tzu, Sun; *The Art of War*, "Chapter 3: Attack by Stratagem"

Optimizing Capability

Previously, it was noted that the question “Is our security program operating effectively?” was a more effective (or at least different) question to ask within the enterprise than “Is my enterprise secure?” Effective operations, after all, encompass more than security.

When optimizing cybersecurity capability, the scope must be holistic and discretely applied. Cybersecurity needs to operate effectively at a micro and at a macro level. At a macro level, the entirety of an enterprise—processes, risk profiles and tolerances, personnel and enterprise culture, and so on—must be taken into consideration, as must external environmental factors, such as the market environment that the enterprise operates within and public perceptions of its actions.[13] A focus on an enterprise’s internal environment should not come at the expense of a focus on its external one; both merit equivalent focus of expertise, resources and concern. At a micro level, individual measures, practices and controls must operate with precision and accuracy; they must be resilient to attack, hardened to circumvention and feed into the broader, holistic risk management strategy.

Operating cybersecurity at macro and micro levels in tandem requires an ability to measure overall resilience—at the macro and micro levels. It has already been noted that organic standards are better tools for this task because they can adapt in response to changes, but even traditional standards can serve a purpose here, providing at least a baseline idea of resilience. No enterprise is impervious to cyberattacks (or the damage that comes with them), but an enterprise with appropriate cybersecurity capabilities is better equipped to address those attacks, mitigate their consequences and return to full functionality swiftly. Underpinning that must be a mechanism to measure the performance and resilience effectively, objectively and reliably.

Operational effectiveness must be optimized to be effective and to retain optimizations over time. To do so requires a commitment to continual improvement of processes and of the effective utilization of resources. New technologies will arise, the threat landscape will morph, shift and then morph again; at the same time, continual improvement must occur to maximize the effectiveness of resources, maintain resilience and ensure that an enterprise’s cybersecurity capabilities retain their robustness.

The twenty-first century marketplace is not like the marketplaces of the nineteenth or twentieth centuries. Threats and opportunities arrive more rapidly: tools, resources and skills so valued a decade ago may have already passed their useful half-life; traditional standards are no longer up to the complete task of providing enterprise safeguards, and find themselves giving way to more organic standards. An enterprise’s cybersecurity capabilities, like its resilience and operational effectiveness, must always be able to evolve and to engage in continual improvement.

[13] Consider, for example, 2010’s “Operation Avenge Assange” in which PayPal and others were targeted with DDoS attacks for freezing customers’ donations to WikiLeaks, etc. For more information: Whittaker, Zack; “Operation ‘Avenge Assange’: How anonymous is ‘Anonymous’?,” ZDNet, 16 December 2010, *http://www.zdnet.com/article/operation-avenge-assange-how-anonymous-is-anonymous/*

A Call to Action

The solutions outlined in this document are not "rocket science." An enterprise can canvass the existing regulatory landscape, guidance and best practices documentation, normalize them against their own risk management concerns and integrate the most-relevant solutions (based on their desired risk postures) into a holistic evolving benchmark. An enterprise can come up with a maturity-and-capability-aware view of each individual control or countermeasure and tie them to the specific risk offset by each. The enterprise can further maintain them so that they are correlated in an ongoing way to new vulnerabilities and changes to the external threat landscape. That said, these mechanisms require effort, work, forethought and discipline to put into practice–resources that an individual enterprise will likely find challenging to spare due to the workaday issues of keeping the enterprise protected and responding to individual threats and incidents.

The pain felt by boards of directors, executives and senior leaders as they seek to refine and hone their security posture—and also as they seek to secure their enterprises against attack—is very real. That pain reflects an asymmetric contest. Attackers have the advantage of time, because they can attack any time of the day or night (or on holidays.) Likewise, they have the advantage of needing only to find the one undefended (or underdefended) place in, for most enterprises, a highly fluid and complicated technical ecosystem. Much like medical practitioners' struggle with uncertainties in diagnosing and treating disease in a human patient because of the complexity of biological systems and the disparate ways in which patients respond to specific treatments, industry must recognize that the complexities in the technical environment are becoming more probabilistic than has ever been the case before. Therefore, cybersecurity-team and business leadership must develop and employ diagnostically relevant tools and methods that direct limited resources into the areas that address the most risk, in the most efficient manner possible.

These organic standards have the capacity to keep up with this changing landscape that traditional approaches do not. They combine with well-understood maturity approaches to create a reproducible, systemic and objective approach. One that embraces flexibility, alignment with risk objectives, and efficacy and efficiency for implementation and measurement. ISACA and CMMI believe that a new mindset among practitioners must be cultivated – to meet the goals and challenges set forth above. This new mindset requires action by enterprises, by the industry and by other bodies like ISACA and the CMMI to realize. Instead of a minimum baseline of effectiveness, this work envisions and delivers a cybersecurity roadmap as an evolving and customizable set of assessments, benchmarks and practices that are driven by an enterprise's risk and can be measured on efficacy, efficiency, maturity and resilience. The industry needs to coalesce around a cybersecurity risk, capability and maturity model, with enterprise-specific data and analyses that are simultaneously actionable and understandable, by every employee and every board member.

The risk that enterprises face in our digital economy is multi-faceted and enormous, and the burdens that boardrooms and C-suites must shoulder because of the enterprise functioning in such a risk-rife environment are onerous. The risk to enterprises is high, and there is a strong sense of urgency—not merely within boards and C-suites, but throughout market sectors and industries—to address that risk. However, the desire and the need for action should not overwhelm the need to ensure the clarity of the threat landscape and, most importantly, the enterprise's ability to defend itself—resiliency.

A society that takes technology for granted and where individual liberties, safety and privacy are protected implies two things: a solid bedrock on which that technology operates and one where enterprises can address security measures in a cost-effective way and a way that is not intrusive to their ability to be economically successful or financially viable.

Acknowledgments

ISACA Board of Directors

Theresa Grafenstine, Chair
CISA, CRISC, CGEIT, CGAP,
CGMA, CIA, CISSP, CPA
Deloitte-Arlington, VA, USA

Robert Clyde, Vice-Chair
CISM
Clyde Consulting LLC, USA

Brennan Baybeck
CISA, CRISC, CISM, CISSP
Oracle Corporation, USA, Director

Zubin Chagpar
CISA, CISM, PMP
Amazon Web Services, UK, Director

Peter Christiaans
CISA, CRISC, CISM, PMP
Deloitte Consulting LLP, USA, Director

Hironori Goto
CISA, CRISC, CISM, CGEIT, ABCP
Five-I, LLC, Japan, Director

Mike Hughes
CISA, CRISC, CGEIT
Haines Watts, UK, Director

Leonard Ong
CISA, CRISC, CISM, CGEIT, CPP,
CFE, PMP, CIPM, CIPT, CISSP,
ISSMP-ISSAP, CSSLP, CITBCM, GCIA,
GCIH, GSNA, GCFA
Merck & Co., Inc., Singapore, Director

R.V. Raghu
CISA, CRISC
Versatilist Consulting India Pvt. Ltd.,
India, Director

Jo Stewart-Rattray
CISA, CRISC, CISM, CGEIT, FACS CP
BRM Holdich, Australia, Director

Ted Wolff
CISA
Vanguard, Inc., USA, Director

Tichaona Zororo
CISA, CRISC, CISM, CGEIT, COBIT 5
Certified Assessor, CIA, CRMA
EGIT | Enterprise Governance of
IT (Pty) Ltd, South Africa, Director

Chris K. Dimitriadis, Ph.D.
ISACA Board Chair, 2015-2017
CISA, CRISC, CISM
Intralot, S.A., Greece

Robert E Stroud
ISACA Board Chair, 2014-2015
CRISC, CGEIT
XebiaLabs, Inc., USA

Tony Hayes
ISACA Board Chair, 2013-2014
CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA
Queensland Government, Australia

Matt Loeb
CGEIT, FASAE, CAE
ISACA, USA, Director

About ISACA

Nearing its 50th year, ISACA® (isaca.org) is a global association helping individuals and enterprises achieve the positive potential of technology. Technology powers today's world and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organizations. ISACA leverages the expertise of its half-million engaged professionals in information and cyber security, governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology. ISACA has a presence in more than 188 countries, including more than 217 chapters and offices in both the United States and China.

About CMMI® Institute

CMMI Institute (CMMIinstitute.com) is the global leader in the advancement of best practices in people, process, and technology. The Institute provides the tools and support for organizations to benchmark their capabilities and build maturity by comparing their operations to best practices and identifying performance gaps. For over 25 years, thousands of high-performing organizations in a variety of industries, including aerospace, finance, healthcare, software, defense, transportation, and telecommunications, have earned a CMMI maturity level rating and proved they are capable business partners and suppliers. CMMI Institute is a part of the ISACA family.
To learn more about how CMMI can help your organization elevate performance, visit CMMIinstitute.com.

Disclaimer

ISACA has designed and created *A Risk-Aware Path to Cybersecurity Resilience and Maturity* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

ISACA®

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Web: www.isaca.org

Provide feedback:
www.isaca.org/CMMI-Cyber-Capability-Maturity

Participate in the ISACA Knowledge Center:
www.isaca.org/knowledge-center

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkd.in/ISACAOfficial

Facebook:
www.facebook.com/ISACAHQ

Instagram:
www.instagram.com/isacanews/