Enterprise Transformation to Cyberresiliency

Serious cyberbreaches with criminal intent and attacks on enterprises are becoming more alarming due to their scale, magnitude of severity and progressive consequences. The average cost of each lost record rose from US $141 to US $148, the average cost of a breach of 1 million records was nearly US $40 million, and the cost of a breach of 50 million records was estimated to be US $350 million. The average time to detect and contain a mega breach was 365 days.[1]

These malicious attacks will continue to trend upward due to the integration of enterprises' supply chain, organizations having a multinational presence, the availability of tools to carry out these attacks, the success and rewards of attacks and, above all, the harm that can be done by attacks that are state sponsored. The risk from devastating cyberattacks is real, and cyberresiliency is warranted.

Cybersecurity is an endless process of chasing and preventing known attacks, anticipating attacks, monitoring, alerting, patching, remediating, and implementing solutions. It is becoming a maintenance function that trails hackers and other bad actors.

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.

Cyberresiliency is the trend of the cybersecurity discipline, at an enterprise level, resigned to the fact that enterprise information technology and systems environments will be severely breached, and it is only a matter of when. The premise of cyberresiliency is to prepare an organization for a devastating cyberattack that could take place and how the possible severity of the breach dictates that enterprises prepare a plan to continue to run its operations at full capacity with a recovery point and time that has minimal impact on its supply chain.

The previous assumptions have elevated the subject of cybersecurity and resiliency to the highest level within the organization, and it is becoming a high-interest topic to enterprise boards of directors (BoDs). This, in turn, positions cyberresiliency as one of the major responsibilities that chief executive officers (CEOs) have to deal with due to the serious consequences that a breach may have on the enterprise and its survival.

Robert Putrus, CISM, CFE, CMC, PE, PMP
Works in information risk management and is a compliance security 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. He 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 *linkedin.com/in/robert-putrus-8793256.*

It is impossible to predict the nature, timing and prevention of all possible attacks. It is becoming more of a mitigation endeavor to prepare a soft landing, as much as possible.

Figure 1 shows key comparative metrics of cyberresiliency vs. cybersecurity.

Measuring Cyberresiliency in an Enterprise

Cyberthreats have been diversified, which requires an alternate defense mechanism to improve enterprises' restoration abilities in the event of major incidents based on the reality that security

Figure 1—Comparative Metrics of Cyberresiliency vs. Cybersecurity

Cyberresiliency	Cybersecurity
It is a business function.	It is of high technical content.
It is a business resiliency.	It is a system resiliency.
It is BoD-focused.	It is senior-management-focused.
It protects the business and ensures business delivery.	It protects the IT environment.
It is a culture of building cybersecurity from within.	It is a mind-set to protect from the outside.
It is a collaborative security: industry and enterprise community.	It is a single-entity focus.
It is understood by business-minded professionals.	It is understood by technical-minded professionals.
The enterprise has the ability to deliver the intended outcome with full capacity.	It reduces the risk of a cyberattack on systems, networks and technologies.
It has the ability to restore regular operations and quickly adjust to circumvent new risk.	It has the ability to recover systems and network technology with some certainty of point and time recovery objective.
The attacks have the element of surprise.	The cyberattacks have predictability of compromise.
It assumes the attackers are superior with innovative tools.	It assumes that the attackers could be circumvented; recovery is a matter of time.
The expected degree of attack has a devastating effect on the enterprise when it comes to continuing its operations. It denies the organization from conducting its normal delivery of operations.	The expected degree of the attack is disruptive to operations.
It is a cultural shift about how organizations think due to the severity of impact.	It is operating the business with expected and manageable risk.
It is planning for the unknown and unpredictable.	It has a high content of predictability.
It encompasses a wider range of organization resources in planning and recovery.	It encompasses smaller resources in planning and recovery.
It integrates IT risk management and business resilience management process (high IT and business management content).	It focuses on IT risk management process (high IT content).
It requires complex planning.	It has less complex planning.
It prepares for absorbing a high-impact attack.	It has a lower degree of absorbing high-impact attacks.
It has extreme recovery procedure.	It is lesser than extreme recovery procedure.
It has a major and proficient range, which scales from process improvement to reengineering.	It has proficient process improvement.
It has a solution, which articulates the principles and the business fundamentals.	It implements solutions of a specific nature, and they will become outdated and obsolete rapidly.
It prepares and fights the unknown while not knowing the unknown.	It fights the known and, to some degree, protects against the unknown.

incidents are neither completely detected nor prevented.

> *Recognizing that 100% risk mitigation is not possible in any complex system, the overarching goal of a risk-based approach to cybersecurity is system resilience to survive and quickly recover from attacks and accidents.*[2]

> “IN SIMPLER TERMS, CYBERRESILIENCY IS THE ABILITY TO PREVENT, DETECT AND CORRECT ANY IMPACT THAT INCIDENTS HAVE ON THE INFORMATION REQUIRED TO DO BUSINESS.”

In simpler terms, cyberresiliency is the ability to prevent, detect and correct any impact that incidents have on the information required to do business. Examples of the enterprise cyberresiliency goals are:[3]

- **Anticipate**—Stay informed and ready to expect compromises from adversary attacks.
- **Withstand**—Continue the enterprise's mission-critical business operations despite a successful attack by an adversary.
- **Recover**—Restore mission-critical business operations to pre-attack levels to the maximum extent possible.
- **Evolve**—Change missions/business functions and/or the supporting cybercapabilities to minimize adverse impacts from actual or predicted adversary attacks; change cybercapabilities for mission-critical business operations to minimize impacts from the actual or predicted adversary attacks.

Vital Signs of Cyberresiliency

A quick diagnostic to identify the readiness of an enterprise to withstand a major cyberattack is through the ability to answer and address the following questions with confidence and truthfulness. These questions should be answered from the “as-is” perspective, i.e., the current readiness of the enterprise:

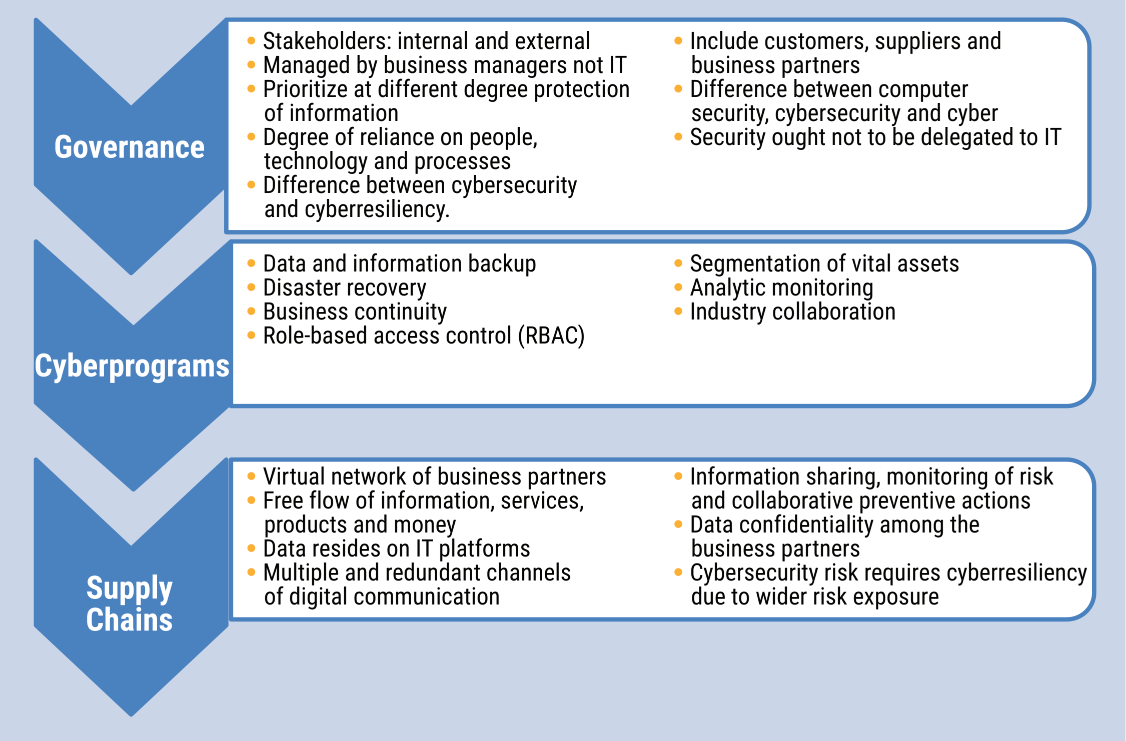
- Is the organization led by legacy business practices and thinking? This is a tone at the top, which will drive the preparedness of the enterprise cyberresiliency. It requires an overhaul of management thinking. Legacy practices slow the transformation and recognition of the need of cyberresiliency, posing a higher risk for enterprises to learn it the hard way. It is, by far, less costly to learn from others' misfortunes.
- In the case of a major attack, how do supply chains and business partners interact and have a free flow of information? For how long could the disruption of the information flow be sustained? The reliance on information is driving competitiveness, which is evolving to be based on ease of flow and sharing information. It is a case of competitiveness and long-term sustainability in question.

Measuring the cyberresiliency of an enterprise is analogous to the four critical vital signs of a human being, which are standard in most emergency medical settings to measure and monitor a person's health. These vital signs are body temperature, heart rate or pulse, respiratory rate, and blood pressure.

Extrapolating the concept of a human being's critical vital signs when a serious emergency occurs to a cyberincident means understanding the vital signs of an enterprise. That is, what is required to sustain and what must be monitored to maintain survival?

The enterprise's vital signs are the degree of effectiveness and compliance with the principles of cyberresiliency, which are governance, cyberprograms and supply chain, and they are summarized in **figure 2**.

Figure 2—The Principles of Cyberresiliency and the Degree Compliance (The Vital Signs)



Governance

- Stakeholders: internal and external
- Managed by business managers not IT
- Prioritize at different degree protection of information
- Degree of reliance on people, technology and processes
- Difference between cybersecurity and cyberresiliency.
- Include customers, suppliers and business partners
- Difference between computer security, cybersecurity and cyber
- Security ought not to be delegated to IT

Cyberprograms

- Data and information backup
- Disaster recovery
- Business continuity
- Role-based access control (RBAC)
- Segmentation of vital assets
- Analytic monitoring
- Industry collaboration

Supply Chains

- Virtual network of business partners
- Free flow of information, services, products and money
- Data resides on IT platforms
- Multiple and redundant channels of digital communication
- Information sharing, monitoring of risk and collaborative preventive actions
- Data confidentiality among the business partners
- Cybersecurity risk requires cyberresiliency due to wider risk exposure

Enablement of Cyberresiliency

Industry standards are emerging to address the issue of cyberresiliency. In 2017, the International Organization for Standardization (ISO) issued ISO 23316, covering the principles and guidelines for organizational resilience for any size or type of organization. The US National Institute of Standards and Technology (NIST) has published a Special Publications (SP) report, SP 800-53, which addresses the resilience of critical national infrastructure.[4] Other trends and perspectives are emerging such as:

- Facing, mitigating and defeating cyberattacks is transitioning from being a single-enterprise event to more of a collaborative effort of enterprises across the supply chain. The risk is propelled to stakeholders, and cyberresiliency has the characteristics of enterprise partnership efforts and industrywide initiatives.
- Enterprises ought to establish principles, goals and objectives in support of achievable cyberresilience metrics.
- There is a shift in business leaders' thinking that an expected astounding surprise attack is a matter of when and not if.
- Managing risk can be optimized and more effective when it combines integration of and reliance on people experience, process compliance and technology hardening. Striking a balance among such players of potential vulnerability is an art, not a science.
- Cyberresilience is a risk-based principle, and it must have the elements of rapid detection and response when major security incidents occur.
- Enterprises ought to examine third-party business relationships in the areas of information technology, systems and cybersecurity using a risk-based management approach.[5]

Hardening Enterprise Cybersecurity

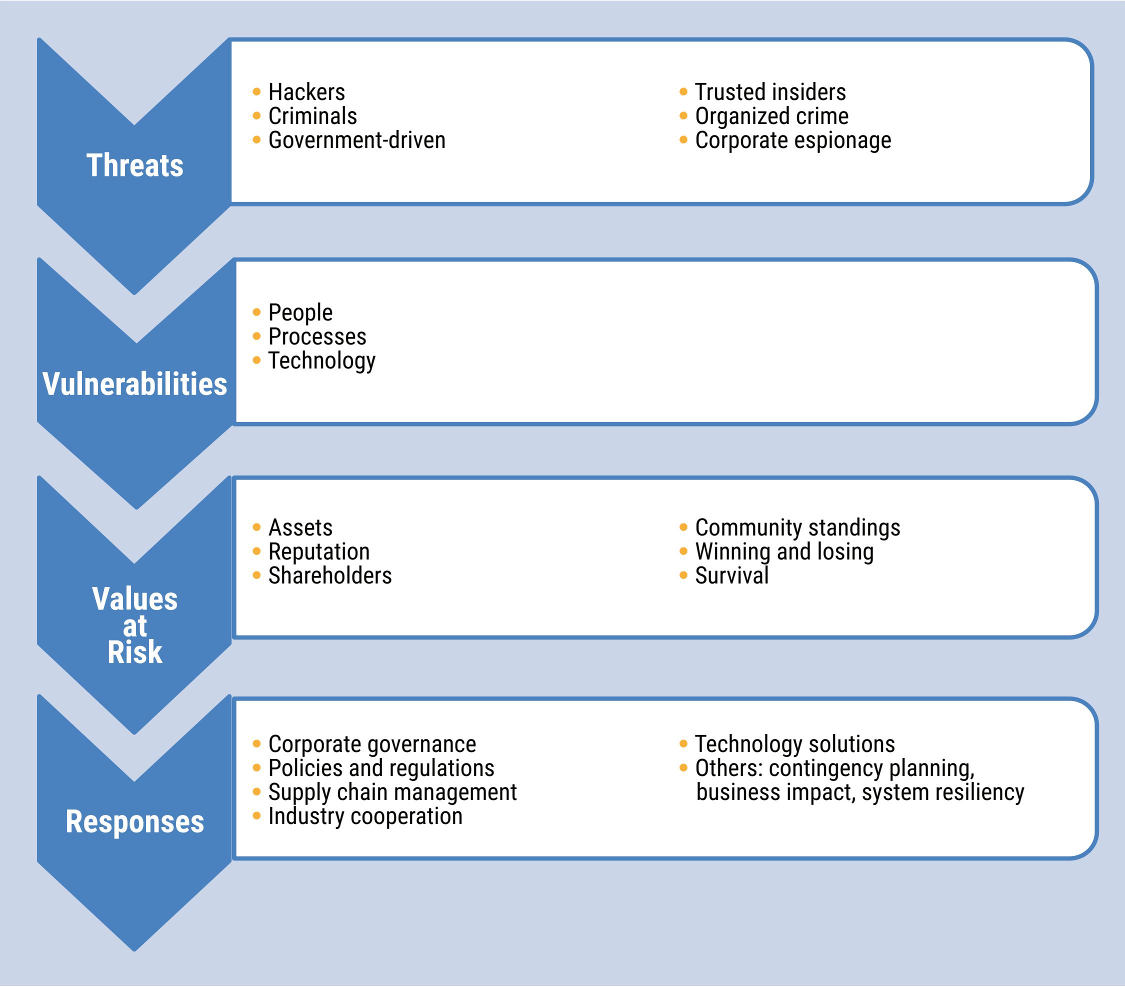
The fundamentals of cyberresiliency represent the "cause and effect" and "action and reaction" expected for an exerted force. Cyberresiliency is based on hardening enterprise cybersecurity, understanding the threats and knowing what are the values at risk. The fundamentals (examples of which can be found in **figure 3**) are:

- **Threats**—Threats have diversified sources based on the motivation of the bad actors.
- **Vulnerabilities**—Sources of vulnerability could be summarized as people, technology and processes. Striking the right balance among these players will achieve resiliency. Relying on one attribute more than another will fracture such resiliency.
- **Values at risk**—It depends on the type of entity the enterprise is, i.e., if it is private, public or government. In addition, there will be a variation of risk with each type of entity. It is critical to have assigned ownership to each vital informational asset within the enterprise.
- **Responses**—Responses can be broken down into contingency planning, business impact and system resiliency.

Quantifying Cyberresiliency Current Status, Preferred Readiness and ROI

Investments in cyberresiliency tend to be significant, so organizations continually seek ways to determine whether the investments are appropriate based on returns. However, enterprises are challenged to apply and fit the traditional discounted cash flow methods to calculate a return on investment (ROI) and justify cybersecurity initiatives. However, cyberresiliency initiatives are even harder to justify than cybersecurity initiatives using traditional accounting methods. Some state that investments in such initiatives are not investments resulting in profit; instead, they address

Figure 3—Hardening the Enterprise and Cybersecurity



loss prevention and mitigation of threats to the organization's assets. In part, this is true. However, in today's world, with the serious impacts resulting from cybersecurity breaches, the argument should be supplemented to state that cyberresiliency is on the same necessity level as any required infrastructure and business units, such as accounting, operations and IT functions that enable enterprises to do business.

A risk tolerance framework could be used to help quantify ROI, but:

> *No mature and recognized risk appetite/risk tolerance framework exists. Also, no quantitative framework for measuring risk is available. There are too many variables to create an acceptably accurate measurement of residual risk. All acceptable models are qualitative.*[6]

Based on experience, there is an absence of suitable tools to use that can quantify cybersecurity risk as attested by professionals, who find that:

> *The need to develop tools to quantify cyberrisk and to assist risk management is well-recognized, as is the current lack of commonly accepted measurement practices.*[7]

An initial focus should be on[8]:

- Multifactor approaches to applicability adoption
- Third-party compliance and substitutability
- Specific scenarios for incident and recovery planning
- Flexible, risk-based governance and reporting principles
- Consensus on methods to quantify cybersecurity risk

The traditional discounted cash flow (DCF) accounting methods are unable to quantify the intangible benefits that cybersecurity and cyberresiliency bring to organizations. In addition, DCF relies on data availability that is quantifiable in nature. But, oftentimes, such data are not available and, consequently, DCF treats cyberresiliency justification as a science. What is needed is the ability to quantify subjectivity through an objective means and base it on management participation and experience.[9]

Cyberresiliency Investment Decision Model: Rationale and Approach

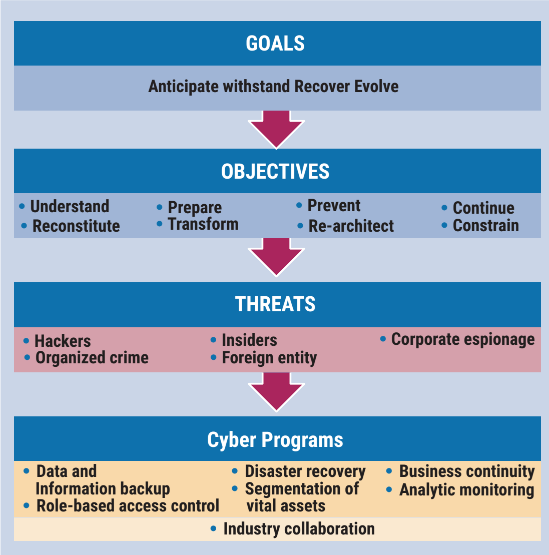
This cyberresiliency model is developed based on a top-down approach with a purpose of quantifying the returns and prioritizes cyberresilience initiatives based on identified goals, objectives and threats. In other words, it seeks to develop the "to-be" state for the enterprise, then enable management to identify the initiatives to close the gaps and prioritize cyberresiliency programs.

The developed prioritization methodology is based on the analytic hierarchy process (AHP) technique to quantify intangibles and prioritize initiatives based on the enterprise business model. The business model is developed through a workshop with the participation of key stakeholders. The top-down enterprise business model is broken down into successive layers (i.e., goals, objectives, threats, cyberprograms) and each layer has its own attributes identified by the stakeholders.

The proposed AHP technique, which is applied to the mock model of cyberresiliency that is depicted in **figure 4**, enables enterprises to quantify the qualitative intangibles and forego any data preparation, and rely solely on the enterprise's key stakeholders' experience building the enterprise business mock model in a workshop session and prioritizing the elements of each identified attribute in the model.

Through this method, organizations are able to build a cyberresiliency decision model (CRDM) as depicted in **figure 4**. It quantifies and compares the degree of impact of each proposed cyberresiliency initiative on any of the enterprise-stated goals and objectives and develops a road map to the containment of the threats. Determining the portfolio of cyberresiliency investment and the realized value of such initiatives is highly correlated to an organization's willingness to articulate the following:

Figure 4—Model of Cyberresiliency Governance



- The risk of potential costs of security incidents that the enterprise is willing to bear
- The level of risk that the enterprise is willing to accept when running its business
- The enterprise's recognition that investment in cyberresiliency ought to be mapped and prioritized to the desired outcome and types of threats

Justifying Cyberresiliency Initiatives

Describing the facilitation process to develop a tailored cyberresiliency model for a given enterprise and AHP method of prioritization is not the focus of this discussion. However, **figures 4-8** are the representation and outcome of such an exercise. **Figure 4** is a mock model of cyberresiliency, which varies from one organization to another, and every enterprise should develop one of its own. **Figure 5** depicts the final score of impact and prioritization of the stated enterprise goals with respect to the governance of cyberresiliency. **Figure 6** depicts the final score of impact and prioritization of the stated enterprise objectives with respect to the governance of cyberresiliency. **Figure 7** depicts the final score of impact and prioritization of the stated enterprise threats with respect to the governance of cyberresiliency. **Figure 8** depicts the final score of impact and prioritization of the stated enterprise cyberprograms with respect to the governance of cyberresiliency, which is required to fortify an enterprise against identified threats.

Conclusion

Cyberresiliency is the extrapolation of cybersecurity, and it has progressed to enable enterprises to withstand and rapidly recover from cyberattacks

Figure 5—Governance of Cyberresiliency: Prioritized by Goals

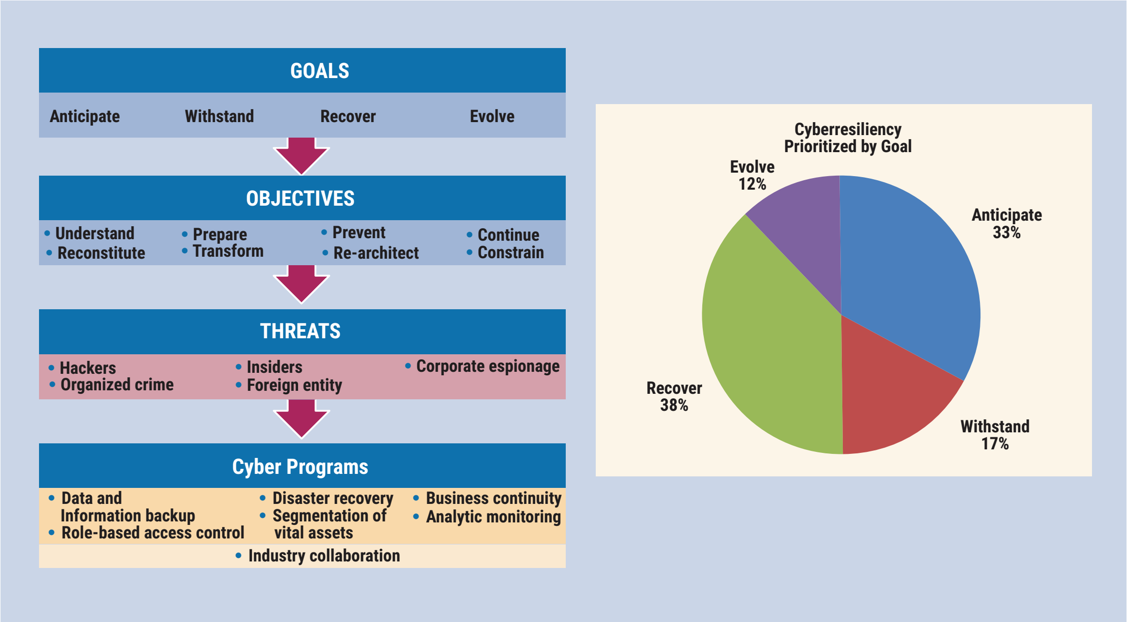


Figure 6—Governance of Cyberresiliency: Prioritized by Objectives

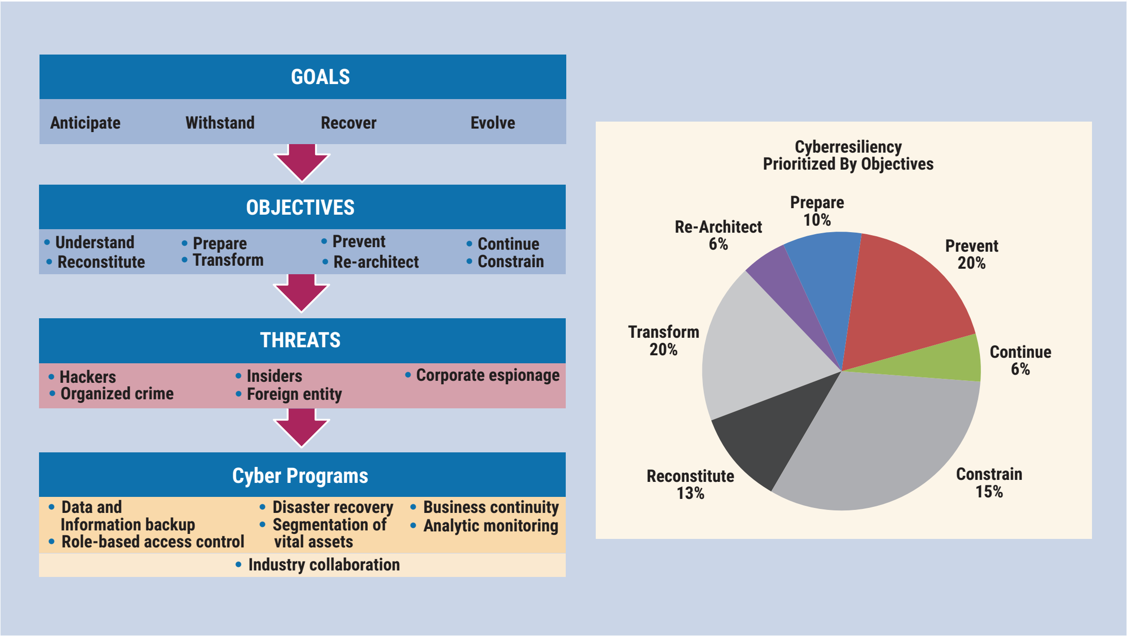
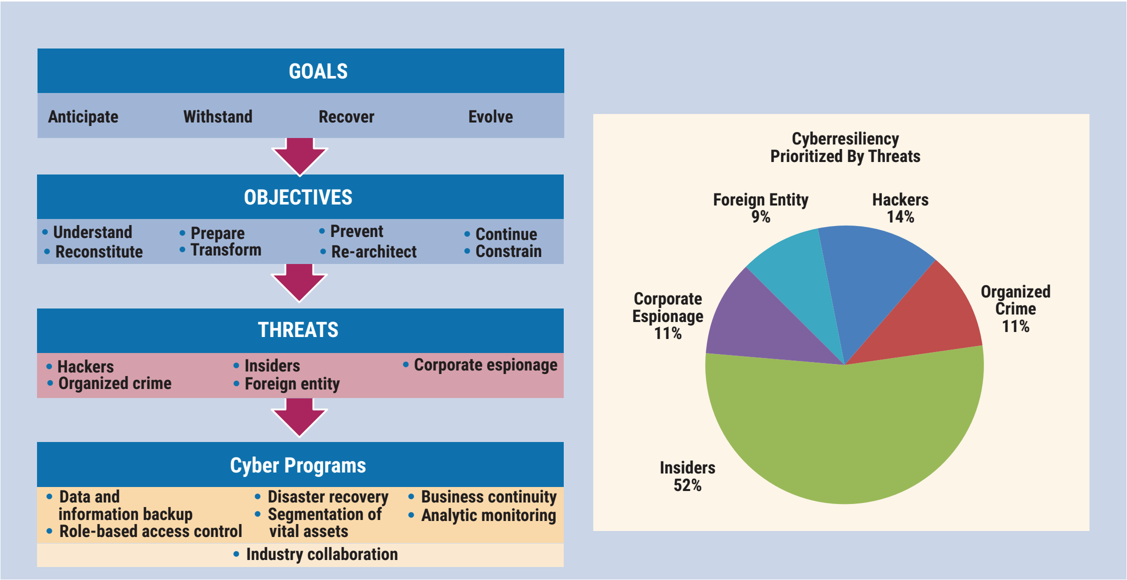


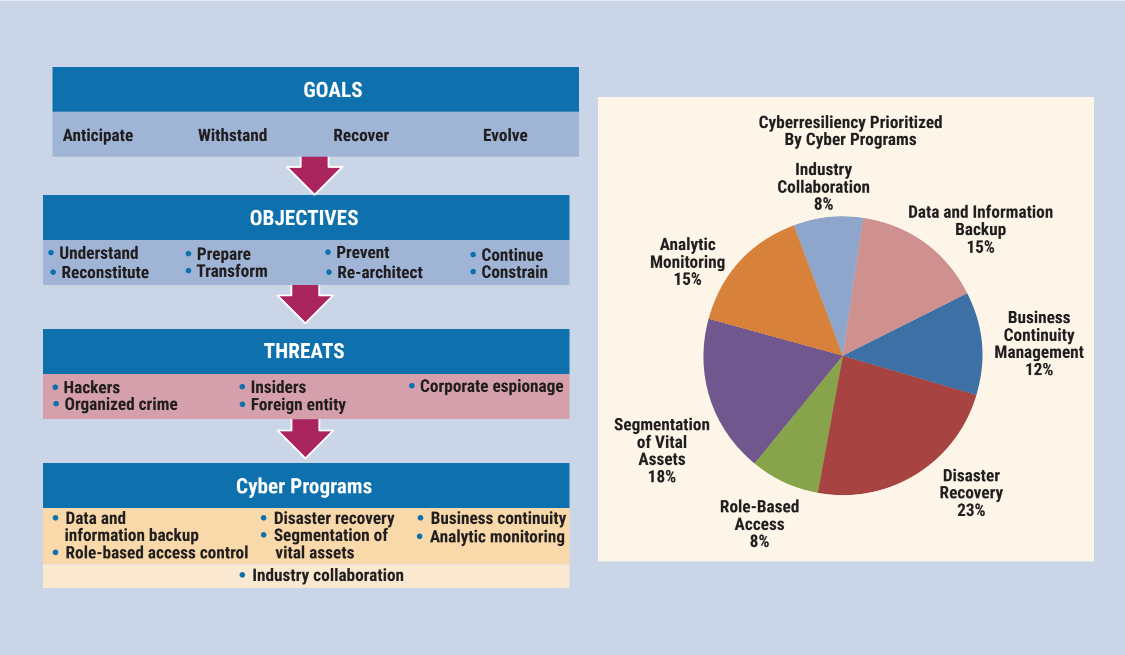
Figure 7—Governance of Cyberresiliency: Prioritized by Threats



with criminal intent to induce harm, cripple and extort enterprises. Cyberresiliency is a board-level responsibility with high business content. It is based on initiatives under the auspices of corporate governance, enterprise cyberprograms and supply chain network.

The trend and severity of serious cyberbreaches brings forward the challenge that enterprises will face a serious breach with intent to harm. The organization and its BoD ought to plan in anticipation of such an attack and how to withstand it, rapidly recover from it, and how to evolve to reengineer its business and cybersecurity processes.

Figure 8—Governance of Cyberresiliency: Prioritized by Cyber Programs



It is the enterprise's responsibility to evaluate and measure its current state of cyberresiliency and how to transform itself to strengthen its cyberenvironment to withstand serious cyberthreats.

Cyberresiliency initiatives are costly. The absence of credible and/or best-fit justification methods represents one organizational challenge. Through the proposed method, the enterprise will be able to identify and prioritize a road map to transform itself to a cyberresilient state.

Endnotes

[1] IBM and Ponemon Institute, "2018 Ponemon Cost of Data Breach Study: Global Overview," USA, July 2017, *https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55017055USEN*

[2] World Economic Forum, "Partnering for Cyber Resilience," 2012

[3] Bodeau, D.; R. Graubart; J. Picciotto; R. McQuaid; "Cyber Resiliency Engineering Framework," MITRE, January 2012, *https://www.mitre.org/publications/technical-papers/cyber-resiliency-engineering-framework*

[4] National Institute of Standards and Technology (NIST), "Security and Privacy Controls for Information Systems and Organizations," NIST Special Publications (SP) SP 800- 53, USA, August 2017, *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft*

[5] Putrus, R.; "Risk-Based Management Approach to Third-Party Data Security Risk and Compliance," *ISACA® Journal*, vol. 6, 2017, *www.isaca.org/Journal/archives/*

[6] US Federal Reserve, "Enhanced Cyber Risk Management Standards, Joint Response from Bank of Montreal (BMO) and Canadian Imperial Bank of Commerce (CIBC)," 17 January 2017, *https://www.federalreserve.gov/SECRS/2017/January/20170124/R-1550/R-1550_011717_131690_286671592059_1.pdf*

[7] US Federal Reserve, "Re: Enhanced Cyber Risk Management Standards," Financial Services Sector Coordinating Council (FSSCC), 17 February 2017, *https://www.federalreserve.gov/SECRS/2017/May/20170518/R-1550/R-1550_021717_131709_429070260162_1.pdf*

[8] *Ibid.*

[9] Putrus, R.; "A Nontraditional Approach to Prioritizing and Justifying Cyber Security Investments," *ISACA Journal*, vol. 2, 2016, *www.isaca.org/Journal/archives/*