Achieving Cyber-Resilience:

A Formula for Success

Wade P. Richmond

At long last, your cybersecurity policies, practices, firewalls, rules, scanners, monitoring, reporting, and other protections are all in place (collective sigh of relief!) Then, a zero-day exploit finds its way into your environment, and your servers begin dropping like flies! The "black hats" have found a way into your network, disrupted your business, and compromised your client, employee, and/or company data … and everyone is looking to you to "fix" everything! Now what?

Well, recent history provides many examples to try not to repeat:

- Sony was hacked and went from being a highly-respected company to the subject of media ridicule for its handling of a cyberattack
- Target, Home Depot, and a plethora of other retailers have been hacked, suffering massive hits to customer confidence that will likely have long-term impacts and potential losses of millions of dollars in sales
- Equifax was hacked and practically bled confidential and personal information, impacting the credit of millions of unsuspecting citizens
- The most recent hack (tentatively attributed to spammers) of Facebook stole the personal information of 29 million Facebook users
- U.S. governmental agencies have been infiltrated by foreign states intent on disrupting service, stealing personal data and credentials, influencing the democratic process, and creating an overall climate of distrust and lack of confidence in "the system"

In all of these cases (and, unfortunately, so many more), executives lost their jobs due to the way they handled these crises, and untold millions of dollars of sales and/or business productivity were lost as well.

Organizations today are confronted by a wide range of cyberattacks, so it comes as no surprise that cyberattacks and data breaches have consistently ranked high on the list of key issues identified for the resilience community according to the DRI International Global Risk and Resilience Trends Reports, issued annually by DRI's Future Vision Committee. This year's report revealed that although the top issues remain the same, there appears to be an even greater focus on technological risk. Given the development of technologies and the growth of business data, this is likely to remain the case moving forward … which may provide new opportunities for hackers to cause such massive disruptions.

If you're thinking that you already know all this, read on. This paper is more than just another statement of the problem. In fact, what you're about to discover is how business continuity and cybersecurity must integrate within every organization. Collectively, these concepts and the resulting action plans will help to develop a strategy to effectively respond to unforeseen events and get your organization back up and running as quickly as possible. They must work in together, however, as they are vital to your organization's ability to survive.

INTEGRATING CYBERSECURITY INTO THE BUSINESS CONTINUITY FRAMEWORK

Clearly, cybersecurity and business continuity must work in concert to streamline well-coordinated identification, respond to attacks or data breaches, minimize costs, and protect the organization's reputation. Here are the specific pragmatic actions required to achieve this integration:

Leadership Involvement

Executing a business continuity plan typically includes having leadership representatives from each area of the business to serve as part of a crisis management team. This group also should be charged with assessing the business impact in case of a cyberattack, and with decisions related to the attack, such as timing of necessary system actions (e.g., a system shut-down). The appropriate organizational leadership must work with the IT team in order to formulate a response strategy and make timely decisions during events caused by any sort of cyber-disruption.

Business Impact Assessment

Does the organization's most recent business impact assessment (BIA) fully identify all critical IT systems, processes, data, and locations that support the organization's revenue, customer information, trade secrets, and other dimensions to ensure a successful business recovery? Identifying all critical parameters of IT-related operations is the first step in mitigating and combating cyberthreats. You must consider reasonable worst-case scenarios to conduct an effective analysis and establish a clear idea of exactly what could happen to the organization if it were affected by a cybersecurity breach.

Risk Assessment

Cyberattacks are a top threat to the business continuity framework of an organization and, therefore, must be assessed appropriately. Cybersecurity is often viewed as an IT issue, which is why it is not surprising that the issue is often seen from an IT-centric perspective, with mitigation strategies based on infrastructure changes, software fixes, etc. In reality, comprehensive risk assessment of an unplanned IT or telecommunication outage due to a cyberattack need to be carried out by IT in coordination with a cybersecurity expert (e.g., the organization's CISO or a contracted resource). Ideally, this would be in consultation with business continuity leadership, in order to arrive at an appropriate technology-associated business continuity framework.

Business Recovery Strategy

When a breach occurs, speed and agility depend on proper recovery strategy design. Results of a BIA, along with risk assessments, must be analyzed by cross-functional teams. This ensures that the persons with the greatest expertise provide the business with technical and administrative knowledge to deal effectively with the situation. Business recovery strategies must be developed, taking the impacts of cybersecurity events into consideration. This will make the organization's business management plans more responsive to cyberevents. The experience of invoking business continuity plans in response to cybersecurity breaches will make future responses more effective.

In addition to best practices to bolster cybersecurity, identifying procedural details of computer backups, data restoration methods, and minimum software requirements are crucial to re-establishing technology and continuity of critical business processes in the event of a cyberattack.

Crisis Communication Plan

Crisis communication plans need to be updated to include external communication that may be needed during cyberattacks. The crisis management team must integrate an organization's official and mandated response for any crisis situation, with specific, timely communication to interested parties. This will help maintain consistency in external communication and ensure that the organization's reputation is well-managed.

Tests and Exercises

Cybersecurity scenarios must be included in business continuity/disaster recovery testing in order to improve the organization's ability to evaluate its cyber-incident preparation, mitigation, response, and recovery capabilities. Periodically conduct a cybersecurity exercise to practice response roles and ensure all communication and decision making is appropriate to control the response and impacts. These types of exercises also can be used to educate staff on technology and business continuity policies and procedures for offsetting cyberattack strategies.

Every organization needs rigorous and regular exercising/testing of integrated business and technology responses to provide assurance that business functions will be able to support restoration or continuity needs. Testing of "defense-in-depth architecture" (multiple redundancies established for IT and telecommunication) is a key consideration during cybersecurity tests and exercises. At the same time, availability of business continuity response plans and manuals for the business recovery team members becomes a key to an effective response mechanism and must be tested during such cybersecurity exercises.

Supply Chain

Cyber-resilience of suppliers is expected to increasingly influence an organization's own cyber-resilience. It is recommended that organizations identify key suppliers, as well as risks associated with those suppliers, to execute continuity strategies in an appropriate manner. Involve key suppliers during any business continuity tests and exercises, in order to seek assurance of contractual obligations and evaluate effectiveness of the business continuity recovery strategy. Equally important is ensuring that suppliers have effective cybersecurity guidelines to prohibit malware from being introduced into the customer environment.

Crisis communication plans need to be updated to include external communication that may be needed during cyberattacks.

CYBER-RESILIENCE: A STEP UP FROM CYBERSECURITY

The world is changing rapidly, and cyber criminals are adapting to it faster than security solutions are being developed. Targeted attacks by skilled and persistent cyber criminals are now a business reality. Traditional security measures such as firewalls and antivirus software are proving inadequate. Since it is widely accepted that it's not a matter of "if" but, rather, "when" an organization will suffer a cyberattack, organizations should assume that they will be breached. Instead of focusing on keeping criminals out of networks, it's more appropriate to assume that they will break through defenses and, therefore, begin working on a cyber-resilience strategy to reduce the negative impact.

For years, those working in cybersecurity fought to elevate the issue to the boardroom. Recent evidence suggests that the message is starting to be heard. According to a study by U.S. consultants McKinsey[1], 75 percent of executives said they considered cybersecurity to be a top priority. Another survey in the UK by KPMG[2] revealed that cybersecurity was very much on the agenda in UK boardrooms, with 74 percent of UK business leaders agreeing that cybersecurity was an enabler of trust and 45 percent believing cybersecurity specialists were an effective part of the business.

Now, we need to gear up for the next battle – convincing organizations of the importance of cyber-resilience. Resilience is one of the most valuable long-term properties of an organization, defining its ability to grow and survive in a changing environment by successfully implementing evolving strategies. As crises are often driven by events that are beyond their control, resilient organizations are those that are best prepared to face and adapt to the challenges ahead.

As the internet of things grows and the adoption of connected devices continues to expand, it's clear that the future holds an even greater dependence on technology. Despite many organizations adopting "digital first" or even "digital only" strategies, few have grasped how dependent core business processes are on the accompanying technology. In the event of disruption or failure, switching to processes that are less dependent on technology is cumbersome, unfamiliar, and often no longer even possible.

Cyber-resilience represents a fundamental change in the way we understand digital technology, risk, and opportunity. As a concept, it is much talked about but can be difficult to define. For the sake of this paper, we will adopt the following (perhaps oversimplified) definition:

Cyber-resilience = an entity's ability to continuously deliver the intended outcome despite adverse cyber-events

Cyber-resilience is a broad approach to cybersecurity – encompassing cybersecurity and business continuity management – that seeks to defend against potential cyberattacks as well as to ensure the organization's survival following an attack. An organization's resilience to cyberattacks is fast becoming a critical survival trait. In fact, the Directive in Security of Network and Information Systems (NIS Directive)[3] is a new EU-wide law that requires organizations operating in critical sectors to achieve a robust level of cyber-resilience. Cyber regulations in the U.S. also have become more stringent and widespread, including the Healthcare HiTech Act in 2009 and financial sector (FFIEC, OCC) regulations that mandate vendor cybersecurity practices. There has even been a trend toward state regulations, such as the New York Department of Financial Services (NYDFS) Cybersecurity Regulation (23 NYCRR 500). The trend toward greater prevention and faster reporting will continue as the pursuit of detection and damage control concerns grows.

In a constantly evolving digital technology environment, organizations must be able to move quickly and seamlessly to adopt new solutions and then detect, evaluate, and hasten resumption of operations, when breaches occur. Organizations need to design business processes and IT systems that protect critical information, implement strong cyber defenses, and establish effective cyberattack response plans.

It is important to understand, however, that cybersecurity and cyber-resilience are not the same thing. Here are a few thoughts on how cyber-resilience compares to cybersecurity and why the two terms cannot be used interchangeably:

Cybersecurity refers to the methods and processes of protecting electronic data, including identifying it and where it resides, and implementing technology and business practices that will protect it. Cyber-resilience is the ability to withstand or quickly recover from cyberevents that disrupt usual business operations. While the terms are similar, to fully understand the difference between these two concepts, consider these two broad characterizations of the different types of cyberattacks: one is meant to affect data, whether it is the theft of data, modification or deletion of data (e.g. ransomware modifying data so it is unusable), and the other is meant to knock an organization offline and/or disrupt regular business operations (e.g. DDOS attack).

It is only appropriate to talk about your cyber-resilience strategy in terms of cyberattacks used to disrupt your operations, not cyberattacks used to steal or modify your data which can only be prevented through a solid cybersecurity program.

It is important to understand, however, that cybersecurity and cyber-resilience are not the same thing.

ACHIEVING CYBER-RESILIENCE

The impacts of a major cyberattack can be devastating. There is no silver bullet to prevent such attacks, and breaches will occur despite preparation and protection. Many organizations lack the sophistication and expertise to address these new threats. To minimize cyberattacks, we must change the way we think about security. We must think in terms of not eliminating cyber-risk but of creating cyber-resilience.

To create cyber-resilience, organizations must change the conversation about cyber-risk. Find and use a common language. It's crucial to align IT with the business and encourage regular, productive discussions to identify the benefits and risks associated with a cyber-resilience strategy. IT security must accept that the business will be tempted to take risks in order to succeed and must empower the business to make informed decisions on managing cyber-risk.

Senior management must take a more active role in establishing and monitoring cybersecurity programs. In a cyber-resilient organization, senior management provides strategic direction and is ultimately responsible for compliance. Educating senior management about the choices they face is key to forming a business judgement that will determine the program's effectiveness.

Additionally, IT must move from a policing mindset to one that promotes an integrated, comprehensive cyber strategy powered by people, processes, and technology. By changing the culture around digital information and nurturing an appreciation for a strategy that encompasses preparation, prevention, detection, response, and recovery, organizations will achieve true cyber-resilience.

In this sophisticated threat environment, traditional security tactics are failing. The old methods of adding another point product to the mix or waiting for IT to identify and propose technology solutions to the business are less effective than ever. No organization can simultaneously sift through voluminous alerts, track vulnerabilities, and apply security policies across various systems and endpoints, while accurately assessing what a mass of global threat data actually reveals in real time. To manage these competing challenges, organizations must change their security posture from a defensive stance focused on malware to a more realistic and resilient approach—a cyber-resilient approach. Additionally, artificial intelligence (AI) is becoming a greater factor in determining the validity of actual cyber-attacks and reducing the number of alerts that may indicate real attacks.

Cyber-resilience is about managing security with a multi-layered approach that encompasses people, processes, and technology. While correlating security intelligence is important, increasing the "security IQ" of your employees is too, helping them make better decisions and reduce risky behaviors. This expanded scope helps eliminate the cyber gap between IT and the business, requiring the two sides of the house to proactively align and present a united front against threat and incursion.

THE FIVE ELEMENTS OF CYBER-RESILIENCE

As threats morph and organizational needs evolve, cyber-resilience must be refined continuously. The context for that refinement process is best thought in terms of five essential elements: prepare/identify, protect, detect, respond, and recover. Using this framework, organizations can evaluate each element of the cyber-resilience strategy. For example, the prepare/identify element includes vulnerability assessments that expose weaknesses in an organization's security posture. By evaluating the risk posed by each weakness and addressing the weaknesses that are most critical, organizations should be able to improve preparedness. With each scheduled cycle of assessments, the security strategy is refined, and since every organization has unique systems and different security needs, the results of each series of assessments should be evaluated based on the current threat environment and the acceptable risk appetite for the organization, rather than a generic series of checklists.

The First Element: Prepare/Identify

To recognize and overcome an attack successfully, it is critical to understand the organization's security and risk posture. Start by identifying and categorizing important information held by the organization. Then, execute an assessment across all infrastructure and information assets against all known security vulnerabilities. Using those results as a baseline for the organization, compare and contrast the results with peer organizations. Remediating obvious concerns will make the organization a less-appealing target for potential attacks.

Invite business leadership to be "part of the team," not just an approval authority. Real engagement from business and data owners during this phase is crucial. Together, rate information assets in terms of value to the business and prioritize what to protect. Ask, where is the data located? Who is using it? What is its value? How is it currently protected? Is it vulnerable? If so, what makes it so? This exercise is a great tool to raise security awareness with employees, as it helps them to see what could happen when their actions place data at risk. Additionally, this joint effort should help to align business and IT relative to cyber-risk and management, while encouraging a cultural change in employee behavior. Specifically, focus on the following:

- Improving visibility and understanding information and systems, through asset and network discovery and mapping
- Understanding cyber-risk posture through assessments and simulations

- Identifying and remediating vulnerabilities in the IT organization, including supply chain, where many cyber criminals originate attacks
- Mapping assets to vendor relationships
- Building awareness of the external threat landscape and understanding how to recognize if the organization is being targeted through comprehensive global threat intelligence, correlation, and analysis capabilities
- Making users cyber-aware through regular and on-going education on best practices and risky behavior
- Ensuring appropriate backup and recovery strategies are in place

The importance of regular training cannot be overstated. Ensure that personnel are aware of existing cybersecurity policies and processes and help them understand the business importance of those policies and processes – as well as their part to ensure success. Employees who are not security-aware, or not aware of the value of the organization's information assets, are particularly vulnerable to a security exploit. All employees must understand appropriate handling of the organization's sensitive information as well as what constitutes employee intellectual property theft.

Once an organization has adopted a policy, created an awareness program, and established access controls, it must implement detection strategies and response plans. A variety of solutions are available to assist, including threat intelligence services and data discovery tools. Threat intelligence plays a vital role in helping organizations prepare for existing and emerging threats.

Security intelligence gives organizations a greater understanding of the entire threat landscape, including threat perpetrators and trends. Scrutinizing internal infrastructure and considering the potential impacts that certain threats can have on the organization allows security managers to proactively predict threats and exploits. As a result, threat intelligence services enable security leaders to better protect and secure their environment and manage risk. As part of the integrated approach, much of this data should be part of the BIA process that identifies the gap between current data and recoverable data.

The Second Element: Protect

Once there's an understanding of what's out there, where it lives, its level of sensitivity, how vulnerable it is, and the organization's risk tolerance, it's time to take steps to protect it. The second element is all about developing and implementing safeguards for critical infrastructure and services in order to limit or contain the impact of a cyberattack. While no amount of time, money, or effort can guarantee success, the goal of cyber-resilience is to minimize the chance of a breach succeeding, and if it does, react quickly to reduce damage.

The infrastructure and information assessment performed should have revealed gaps in existing defenses. But how well-maintained and up-to-date are existing prevention solutions? Are defenses prepared to protect against the latest advanced threats or innovative exploits? Is the organization relying on disjointed point products? Is there an integrated approach to protection that provides effective situational awareness and the ability to better respond to cyber-risks? Are there policies and automated enforcement in place to minimize human factor or process-related breaches? How about a feedback loop to improve outcomes? In particular, focus on protecting and securing:

- Website and online users from cyberthreats
- Business-critical systems from cyberthreats (the data center is typically the best place to start)
- Endpoints and gateways from targeted attacks and advanced threats
- Mobile workforce and customers
- Information assets over their lifecycle, including protection from data loss or illegal access (consider encryption or using a data vault)

All three areas – people, processes, and technology – are important to the protection element. The necessary technology must be in place to safeguard critical infrastructure and assets. The technology solutions employed also must offer protection for an increasingly mobile workforce. Safeguarding mobile access to the network and data is becoming more and more important as employees' ability to access sensitive corporate information increases. In addition, technology must be integrated to provide the intelligence that will allow for quick detection of any cyberattack.

Managing people and processes is essential. A recent Ponemon Institute study[4] found that 35 percent of the root causes of data breaches involved human factors, such as negligent employees or contractors. The same report attributed 29 percent of breaches to system glitches, including IT and business process failures. Breaches related to human factors or process failures may be driven by employees' lack of appreciation for cybersecurity. Inappropriate use, storage, or distribution of the organization's sensitive information and a lax approach toward operational and business policies are often at the root of human error.

THE FIVE ELEMENTS OF CYBER-RESILIENCE

As threats morph and organizational needs evolve, cyber-resilience must be refined continuously. The context for that process is best thought of as a structure with five elements:

The First Element: Prepare/Identify

- Implement asset/ network discovery and mapping
- Understand cyber-risk posture
- Identify/remediate IT vulnerabilities
- Map assets to vendor relationships
- Build awareness of the external threat landscape
- Increase cyber-awareness through education
- Ensure backup and recovery strategies are in place

The Second Element: Protect

- Secure website and online users
- Protect business-critical systems
- Secure endpoints/ gateways
- Protect mobile workforce/customers
- Safeguard information assets

The Third Element: Detect

- Implement detection strategy
- Assess affected systems
- Ensure timely response
- Monitor related attack indicators
- Ensure effectiveness of safeguards
- Consider managed security offerings
- Correlate security intelligence

The Fourth Element: Respond

- Measuring and track cyber-resilience
- Outline response to cyberattack
- Establish response processes maintenance/ testing
- Coordinate communications response activities
- Incorporated lessons learned

The Fifth Element: Recover

- Develop/implement data restoration plan
- Understand backup content and importance
- Ensure communication with data centers
- Consider factors unique to cyberattacks
- Ensure critical system availability

In addition to education and awareness, organizations must monitor and enforce policy adherence. Not only does policy enforcement and monitoring improve an organization's risk posture, but it also conveys to the entire workforce the importance the organization places on its confidential information and intellectual property. A lack of policy enforcement and monitoring creates a cultural attitude with the opposite effect – if IT doesn't value and protect digital information, why should employees?

The Third Element: Detect

The detect element focuses on developing and implementing activities to identify an attack rapidly, assess the systems that may be affected, and ensure a timely response. In addition, this stage is concerned with continuing to monitor the network for related attack indicators and ensuring the effectiveness of safeguards. A critical downside of an organization spending so much time and effort trying to protect itself from attacks is that the entity often fails to prepare for what to do when an attack succeeds. One of the most significant consequences of this lack of preparation is that it cripples the organization's ability to effectively respond to the breach.

As response time and time to resolution increase, cyber criminals have more time to exploit and damage the business. With the total cost per data breach incident in the U.S. now at $3.86 million on average, this is no small problem. Damages not only include the cost of remediating the breach but also penalties for non-compliance, loss of reputation, and/or loss of customers. Of course, if the organization lacks the solutions to detect the breach in the first place, the cyber-criminal can wreak havoc indefinitely.

When a breach occurs, the only way to minimize damage is to have detection and response policies, processes, and technologies in place. While many organizations already have detection and response strategies, they must regularly evaluate if these are adequate and determine if they are able to contain and remediate breaches faster. Big data and associated analytic tools coupled with the emergence of cloud, mobile, and social computing offer opportunities to process and analyze structured and unstructured data related to cybersecurity to help with this process.

Think about how to monitor internal security events and correlate them to external threats, as well as how to make sure the data is readily available to determine when or whether a breach has occurred. Monitoring potentially hundreds of endpoints, logins, and data access attempts on a busy network is no simple task. When combined with maintaining awareness of the global threat landscape, it's impossible. This is where a managed security service can be helpful. Managed security offerings range from security monitoring and prioritization to advanced threat protection and incident response management. They can help to build a resilient security strategy that allows organizations to better prepare, protect, and respond to complex cyberattacks.

All cyber-resilient organizations create a proactive IT department with visibility across the entire environment – one with deep, data-level integrations that yield insight, and that evolve and respond as attackers become more advanced. By correlating security intelligence, IT can detect and remediate a potential issue before it spreads, resulting in reduced damage and cost.

Clearly, the objective is for breaches to be detected before they are identified by internal operations and customers. Reduced latency time—the actual time of a breach to the time the organization recognizes that there has been a penetration—is the goal. The significance of this problem is detailed in 2018 Cost of a Data Breach Study: Benchmark research sponsored by IBM Security independently conducted by Ponemon Institute LLC, which found that the mean time to identify (MTTI) was 197 days and the mean time to contain (MTTC) was 69 days. Both the time to identify and the time to contain were highest for malicious and criminal attacks and much lower for data breaches

caused by human error. Organizations that identified a breach in fewer than 100 days saved more than $1 million as compared to those that took more than 100 days. Similarly, those that contained a breach in fewer than 30 days saved over $1 million as compared to those that took more than 30 days to resolve. This is what separates cyber incidents from normal disruptions, which are almost immediately identifiable.

The Fourth Element: Respond

The respond element provides guidance on the types of activities that can decrease the time to begin remediation and contain the impact of the attack once detected. For the detection process to have value, there must be a timely response. While there are many solutions and services available, much of what is needed in terms of response involves people and processes internal to the organization.

Organizations need a response plan that tells people what to do when an incident occurs. A Computer Security Incident Response Team (CSIRT) should be established and integrated into the BCM incident management team, with specific roles and responsibilities identified. A team leader/manager should be appointed and assigned the responsibility of declaring an incident, coordinating the activities of the CSIRT, and communicating status reports to upper management.

Having a pre-defined action plan that is understood by everyone helps coordinate response efforts. A response plan enables you to determine the extent of the risk to the environment and respond. For the quickest response, automating the remediation steps is ideal — in addition to exercises during which employees practice executing policies and procedures. In developing the plan, focus on:

- Managing risk by measuring and tracking cyber-resilience, including how well systems were protected during an attack (is there infection or was the attack repelled?)
- Creating an outline for the intended response to cyber incidents
- Determining how response processes and procedures will be maintained and tested
- Coordinating communications response activities and understanding how analysis and mitigation activities will be performed
- Devising a system whereby lessons learned are incorporated into future response activities

It can be difficult to remediate an attack. Organizations are effectively, and in some cases literally, held ransom when an attacker gains control of their systems. Two recent incidents demonstrate the impacts upon critical service organizations:

- In Mecklenburg County, NC, online systems and applications were compromised in a ransomware attack that left more than 80 internal and public-facing online systems inoperable. This included vital emergency services.
- Hollywood Presbyterian Medical Center paid a $17,000 ransom in bitcoin to a hacker who seized control of the hospital's computer systems and would restore access only when the money was paid, rendering all medical systems inoperable.

The good news is that ransomware is instantly identifiable and can be remedied by paying a relatively small sum. The bad news is that ransomware breach techniques can later lead to data theft.

The Fifth Element: Recover

The final element that needs to be addressed is recovery. Recover involves developing and implementing systems and plans to restore data and services that may have been impacted during a cyberattack. Even if you respond quickly to a cyber breach, an attack may have consequences. No matter the outcome, organizations must be able to restore their people, processes, and systems as quickly as possible. An effective recovery depends on a clear and thorough recovery plan.

Many organizations already have business continuity and disaster recovery plans that include elements such as backup and recovery, cloud storage, off-site archives, redundant and geographically separated data centers, and other business continuity measures. However, these plans often fail to cover essential recovery practices and scenarios.

For example, while most organizations perform regular backups, very few actually know what they're backing up. It's important to understand how much of the information being backed up is genuinely important to the business. If a disaster occurs, what information and systems must be restored first to return to normal operations? Organizations must ensure that recovery plans answer these questions. Equally important is to ensure that backups are secure. The easiest way to paralyze an organization is to corrupt the backups first and then corrupt the primary data, rendering restoration impossible.

Redundant data centers are important, but keep in mind logistical and geographic considerations that may affect failover ability. Data centers in close proximity to one another, for example, won't help if a major catastrophe hits an entire city or region. Aside from geographic considerations, what happens if an emergency wipes out communication with the data centers?

If a massive cyber breach occurs, organizations need a plan of action for resuming normal operations. Many organizations with comprehensive, traditional business continuity plans and regular recovery and data center failover drills were woefully unprepared when hit with an enterprise-wide cyberattack.

Think about how a cyberbreach would affect systems, people, and processes. What will be needed if employee's smartphones or tablets are compromised? If an aggressive malware attack renders a significant number of laptop hard drives unusable? How quickly can new hard drives be rebuilt? Are there processes in place to provision new systems quickly for essential employees if needed? Think through all the ways a cyberattack may impact the organization. What processes and procedures are needed to recover from them?

Critical systems must be available during an incident; decide how to restore other systems and data afterward. As with response plans, re-evaluate and update recovery plans regularly.

No matter the outcome, organizations must be able to restore their people, processes, and systems as quickly as possible.

A FORMULA FOR CYBER-RESILIENCE

Many strategies may be considered in order to achieve cyber-resilience; however, this paper will present a simple formula made up of the five elements previously explored. The formula groups the elements into two areas (cybersecurity vs. business continuity) as follows:

Cybersecurity = Identify, Protect, and Detect

Challenge: The first phase of a cyber-resilience program involves being able to effectively identify, assess, and manage the risks associated with an organization's network and information systems, including those across the supply chain. It also requires the protection of information and systems from indeterminate cyberattacks, system failures, or unauthorized access. A robust cyber-resilience posture further requires continuous monitoring of network and information systems to detect anomalies and potential cybersecurity incidents before they can cause significant damage.

Solution: Implement an information security management system (ISMS) and conduct regular penetration testing. An ISMS is a system of processes, documentation, technology, and people that helps to manage, monitor, audit, and improve the organization's information security. It helps manage all security practices in one place, consistently and cost-effectively. Combined with regular penetration testing, ISMS will significantly improve information security defenses and reduce the risk of a cyberattack.

ISMS Benefits:

- Secures information in all its forms
- Protects the confidentiality, integrity, and availability of data
- Offers organization-wide protection
- Safeguards against evolving security threats

Business continuity = Respond and Recover

Challenge: The next phase of developing a comprehensive cyber-resilience program is to create response capabilities and integrate them into the incident management phase of the business continuity management plan. These response and recovery measures will help minimize the impact of an attack.

Solution: Implement a business continuity management system (BCMS) and integrate the cybersecurity incident response management program.

A BCMS is a comprehensive approach to organizational resilience. BCMS involves managing risks to ensure that mission-critical functions continue to provide an acceptable level of service, even in the event of a major disaster. By incorporating a comprehensive cyber-incident response management program, a complete BCMS will ensure rapid response and recovery.

BCMS Benefits:

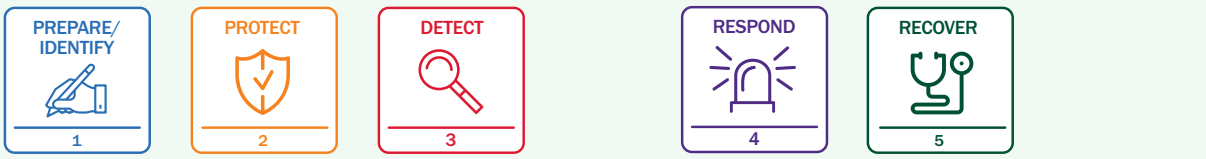
- Maintains continuity of business operations
- Significantly reduces the time to identify and contain the data breach incident
- Reduces the cost of business interruption
- Minimizes disruptions to business operations when a data breach occurs
- Expands the risk assessment process to identify cyber weaknesses
- Ensures a fast recovery after a breach
- DR automation and orchestration reduces the per day cost of a data breach
- Using this simple formula, organizations can achieve cyber-resilience (see page 14 for an example of a cyber-resilience-by-design mapping).

IN CLOSING

Due to a powerful combination of influences, the workplace is changing at an exponential rate. In its Nexus of Forces[7], Gartner defines this phenomenon as "the convergence and mutual reinforcement of four interdependent trends: social interaction, mobility, cloud, and information" that "combine to empower individuals as they interact with each other and their information through well-designed ubiquitous technology." Increasingly dependent on connectivity, we're using the web to get work done in real-time by connecting to the Internet and mobile devices. Both empowering and greatly disrupting, these converging trends are making business more competitive and agile – yet also more vulnerable to cyberattack – and organizations are struggling to stay abreast of the challenges they raise. In this environment, a thoughtful strategy to integrate both cybersecurity and business continuity plans into an enhanced cyber-resilience program is the key to success.

A FORMULA FOR CYBER-RESILIENCE

Follow this simple formula (cybersecurity + business continuity) to achieve cyber-resilience.



Cybersecurity (Elements 1-3)

1. Identify, assess, and manage the risks
2. Protect information and systems
3. Detect anomalies/cybersecurity incidents

Business Continuity (Elements 4 and 5)

4. Respond with proven capabilities
5. Recover via incident management plan

FIGURE 1 Example of resilience-by-design approach mapped across resilience checkpoints of an organization

Checkpoints for Resilience		Threats		Opportunity	
Category	**Resilience Issues**	**Potential Crises**	**Traditional Risk Approach**	**Opportunities for Improvement**	**Resilient Approach**
Digital Infrastructure Management	Ability of organization and external suppliers to ensure continuity of systems availability and a lack of reversionary modes	Systems become unsupported Problems in upgrading Unable to recover systems	Map systems and networks Vendor assessment Contractual agreements Upgrade policy (e.g. Upgrade to the x-1 version)	Reduce digital complexity and failure points Eliminate legacy systems and costs Switch to new rather than recover where advantageous	Create IT roadmap Map core processes Map systems and networks Identify vendor vulnerabilities Contingency plans to accelerate change vs recovery
Cloud Technology	Organization becomes networked into the supply chain issues and vulnerabilities of the system provider	Issues in supply chain of cloud providers are not transparent Cloud outages	Business continuity, contingency and disaster recovery processes Contractual agreements Vendor assessment	Use of cloud technology offers better availability reliability and security over in-house systems Plan for crisis	Identify core process and cash flow vulnerabilities Develop digital workarounds and alternative for core processes
Information Storage and Recovery	An organization is increasingly dependent on its data and code in order to survive	Data is unable to be recovered in the event of a major outage	Disaster recovery process Business continuity planning Crisis planning	Ensure data can be recovered even with loss of system Structure data to migrate onto alternative system in event of extended outage	Simplify data as far as possible Ensure separation between systems and data for core processes Evaluate alternative highly scalable platforms
Insider Threat	Deliberate misuse, or lack of security awareness, by individuals exposes organization to malevolent attack	Fraud Ransomware Cyber-attack / terrorism Staff use unauthorized work-around systems	Risk assessment Compliance training Periodic permission reviews	Develop organizational competencies and values around customer privacy and security	Risk mitigation maturity matrix Map responsibilities Consider permission resilience issues Crisis testing
Communications	Ability of organization to survive from loss of communications (e.g. corporate telecommunications provider)	Degraded organizational capability Isolated employees and poor decision making in crisis	Contractual service agreements	Respond more quickly than competitors Prioritize key decision-making personnel and processes Concentrate on what needs to be done to maintain cash flow	Identify key personnel and core decision making processes Determine order for recovery Develop alternative communication tools for differing scenarios
Networking Within Digital Infrastructure	Platform technology, internet- of-things, and APIs	These technologies improve capability and ease of use, but can introduce vulnerabilities	Antivirus software	Take advantage of network capabilities but prevent/limit contagion by intelligent design	Map core systems and processes Design to create smaller isolated networks wherever possible

Checkpoints for Resilience		Threats		Opportunity	
Category	**Resilience Issues**	**Potential Crises**	**Traditional Risk Approach**	**Opportunities for Improvement**	**Resilient Approach**
Trusted Software	Auditability of the purpose, status and provenance of all software used by the organization	Susceptibility to software failure or cyber-attack (by internal and/or external agents)	Contractual liability Vendor assessment Employee vetting	Certify products and services as trusted Establish leading position in marketplace for trust and reliability	Develop criteria and process for trusted software Establish audit methodology for releases
Machine Learning	Algorithms are being used to make increasingly complex decisions but can reinforce bias in decision making (e.g. ethnicity bias)	Unprofitable decision-making PR and ethical problems (e.g. bias affecting minority groups)	Encourage diversity in coding team makeup Spot sampling and analysis of decisions	Make more consistent decisions Transparency in policy and decision-making processes available to regulator Position in market place as trusted company	Code versions available for regulatory inspection Publication of criteria used
Cybersecurity and Terrorism	Attack on digital infrastructure by outside forces	Fraud Ransomware Loss of core systems affecting cash flow Breach impacting regulatory compliance (e.g. PCI, GDPR, HIPAA)	Cyber war rooms Monitoring systems	Create resilience culture within team Reassess threat in line with business activity and profile Minimize attack surface	Assess triggers and potential scale of threat to location, company and industry based on activity Create a life-long learning organization
Political/Economic/ Societal/ Technological	Long term trends and conditions that impact the business model	Profitability Existential threat	Annual strategy review	Re-engineer the company to adapt to new technology Avoid existential threats	Assess effects outside the analytical window of strategy processes Be prepared to 'destroy' the company to 'save' it
Location	Specific conditions (non-catastrophic) affecting the principal business conditions	Productivity issues (e.g. supply chain problems) Business continuity in event of major incident	Ad hoc solutions Business continuity planning	Change organizational model and processes to maximize advantages and minimize disadvantages	Determine issues Develop measurements and review processes Utilize technology to work around or eliminate issues
Natural Disaster & Climate Change	Catastrophic event (e.g. an earthquake in Silicon Valley)	Scarcity of essential resources cause short term disruption (e.g. running water, communication outages, etc.) Business continuity issues in medium to long term	Insurance Disaster recovery process Business continuity planning Crisis planning	Plan for certainty of event Take advantage of lower asset prices in safer locations (sooner vs. later)	Map core processes and assets Redesign organization Relocate and protect core operational processes and assets

End notes:

1 McKinsey & Company, A New Posture for Security in a Networked World, March, 2018

2 KPM, Staying Ahead of Cyber Crime, April, 2018

3 European Commission, Directive in Security of Network and Information Systems (NIS Directive), July, 2016

4 The Ponemon Institute, The Human Factor in Data Protection, January, 2012

5 IBM Security & Ponemon Institute, Examining the 2018 Cost of a Data Breach, July, 2018

6 Verizon Enterprise Solutions, 2014 Verizon Data Breach Investigations Report, April, 2014

7 Gartner, Nexus of Forces, August, 2014