MITSloan
Management Review

RESEARCH HIGHLIGHT

An Action Plan for Cyber Resilience

It's impossible to avoid all cyber risk. Here's how to make your company more resilient in the face of new threats.

Michael Coden, Martin Reeves, Keri Pearlson, Stuart Madnick, and Cheryl Berriman • January 04, 2023

Reading Time: 11 min

The NotPetya malware attack of 2017 encrypted the systems and disrupted the operations of global businesses, starting in Ukraine and spreading rapidly to over 60 countries around the world. Global shipping company Maersk, one of the worst hit, ultimately needed to rebuild its entire IT infrastructure. In the nine days it took to get its systems back online, the company struggled to continue operations using manual workarounds that teams came up with on the fly. In the end, the incident cost Maersk nearly $300 million.

A more recent ransomware attack shut down the operations of JBS USA, the largest U.S. meatpacker, and other attacks have affected hundreds more companies. In late 2021, for instance, the Log4j vulnerability allowed adversaries to embed malware and take control of millions of Java applications developed over the past decade. These widespread incidents have proved that successful cyberattacks are inevitable.

Given that it's impossible to protect against all new cyberattacks, it has become critical for companies to reduce the impact of cyber breaches by focusing on cyber resilience. Cyber resilience requires a systematic, structured, adaptive approach and cannot be relegated to the office of the CIO or chief information security officer. Because it potentially involves all parts of the business, it must be led by the C-suite and board.

Traditional Cybersecurity Is Insufficient

Most organizations evaluate their cyber maturity according to the National Institute of Standards and Technology's Cybersecurity Framework, but it is 80% focused on identification, protection, and detection, and only 20% on an organization's ability to respond to and recover from a breach.[1] Similarly, our research on cybersecurity spending shows that

72% is spent on identification, protection, and detection, with only 18% spent on response, recovery, and business continuity.[2] Not only does this imbalance leave organizations vulnerable, but it leaves companies ill prepared to comply with new rules proposed by the U.S. Securities and Exchange Commission that would require companies' SEC filings to include details on "business continuity, contingency, and recovery plans in the event of a cybersecurity incident." Cybercrime laws have already been enacted in 156 countries, and 250 bills are being considered in 40 U.S. states and Puerto Rico, with additional cyber resilience regulations expected to follow.

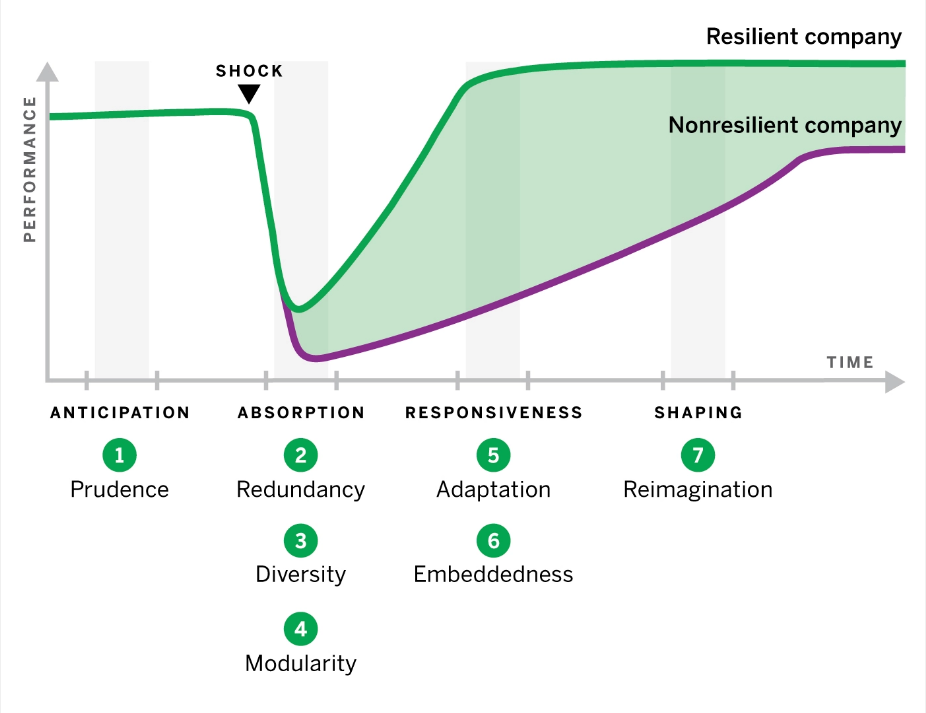
Cybercriminals are well financed, highly organized, and innovating at a much faster pace than cyber protection. Cyberattacks are now endemic, and it is important for each company to build resilience against unavoidable threats, just like our bodies do to fight an endemic disease. The flu and COVID-19 vaccines can help our bodies strengthen our immune systems to protect our vital organs; likewise, management can employ adaptive thinking to build effective cyber resilience for companies' critical systems — for both known and unknown threats.

A Strategic Framework for Cyber Resilience

A cyber-resilient company that rapidly regains its performance capabilities after a shock operates on four distinct time scales (anticipation, absorption, responsiveness, and shaping) using seven adaptive design principles: prudence, redundancy, diversity, modularity, adaptation, embeddedness, and reimagination.[3] (See "Design Principles for Organizational Resilience.")

Design Principles for Organizational Resilience

This framework for building a measured and managed cyber-resilient organization is based on actual data from the responses of U.S. public companies to disruptions, such as economic downturns and the COVID-19 pandemic, over the past 30 years.



Source: BCG Henderson Institute

Anticipation: Before the Breach

1. The principle of *prudence* tells us that if something can go wrong, it eventually will — including everything we think will *not* go wrong. We must expand our ability to anticipate, focusing not only on known cyberthreats but also on how to respond and recover critical business functionality if systems are disrupted by cyberattacks not yet invented. When a breach occurs, the cyber-resilient enterprise continues operating with little or no disruption to its mission, in the same way that a football team adapts its well-practiced defensive plays in real time to the offense of the opposing team, without waiting for detailed instructions from the coach.

The most effective way to start developing prudence is with tabletop exercises (TTXs). Too often, TTXs focus on the incident response to the cyberattack, and only the cybersecurity incident response team and a crisis management team are involved. Involving only these two teams in the TTX is equivalent to having the fire marshal conduct a fire drill without employees participation. Just as organizations require all employees to practice fire drills, prudence instructs that all employees, including those from supply chain, operations, sales, customer support, finance, HR, IT, and administrative services, must know and practice their roles in cyber resilience.

In a TTX we conducted in 2018, we imagined a cyberattack scenario in which a media company's facilities were unusable, requiring all employees to work remotely. Company management said such a scenario could never happen but proceeded to humor us, developing a recovery plan for that seemingly impossible scenario. One year later, COVID-19 forced all of the company's employees to work remotely. The company was able to respond relatively quickly to the shift to remote work and somewhat minimize business disruption, because the managers of many departments — including operations, administration, legal, HR, and finance — had practiced for this unthinkable situation. There would have been even less disruption if more employees had practiced.

Absorption: Reducing the Immediate Impact of the Breach

Cyber-resilient organizations have three interdependent levers for absorbing the impact of the cyber breach: redundancy, diversity, and modularity.

2. *Redundancy* includes both duplicate elements (such as multiple data centers or cloud instances, and multiple factories that could produce the same product) and buffering to compensate for shortages that might occur (such as increased inventories of raw materials, work in progress, and finished goods). These two capabilities are taken from biology, where complex organisms have, for example, multiple redundant antibodies and a store of fat off of which they can live if there is a shock to their food supply.

Redundancy applies to human operations, not just technical processes. Do employees have alternate processes for continuing business operations? When Maersk was hacked, the computer systems routing billions of dollars of goods were rendered unusable for weeks. Luckily, institutional memory allowed it to reinstate its pre-digitization paper-based system.

Ensuring that the workforce has redundant ways of working helps resilient organizations absorb an attack.

3. *Diversity* harnesses the power of heterogeneity in people, processes, and systems. When all operations use the same technology, they can all be compromised simultaneously. Diverse systems, applications, data centers, clouds, operations, manufacturing methods, communications systems, and workforce procedures enable the organization to absorb and reduce the magnitude of the impact of a cyber breach on the enterprise.

Communications during a cyber event illustrate the point. Typically, either email is no longer functional or, if it is, the adversary is reading emails and thereby staying steps ahead of the defense. Diverse and secure communication methods across various stakeholder groups — employees, suppliers, customers, shareholders, law enforcement, and regulators — are critical for the organization to be able to absorb the attack and continue business operations.

Many companies prioritize cost efficiency, using a single, common system throughout the enterprise for each major function. While this approach might reduce short-term operating costs, it can greatly increase the financial impact of a cyber breach.

Resilient organizations acknowledge and manage the trade-off between reducing daily operating costs and cushioning the impact of a cyber breach by employing diverse systems and human procedures. This can be challenging, because the benefits of efficiency are noticeable and immediate whereas the cyber resilience benefits of diversity are obscure and latent. In our experience, the proper balance can be achieved only when cyber resilience is made an explicit priority.

4. *Modularity* refers to the possibility of isolating compromised systems from healthy systems and substituting healthy systems to perform the critical enterprise functions of compromised systems.

Isolation is a common focus of cybersecurity today in zero-trust architectures, network segmentation, and least privilege access management.[4] These approaches often prevent cyberattackers from moving from compromised systems to healthy systems or from gaining access to the most business-critical systems. However, isolation as it is practiced by many organizations focuses only on protection, and cyberattackers are constantly innovating new ways around these defenses.

Cyber-resilient organizations develop digital systems that allow for rapid component substitution, enabling critical business functions to be restored by substituting a healthy system — one that might not be an identical replacement — for a compromised one. Borrowing from human biology, when one muscle is injured, other muscles compensate. One early indication of resilience by design is DBOS, a revolutionary operating system that self-detects cyberattacks in milliseconds and then rolls back to the pre-attack state for business continuity in seconds, without requiring complex, lengthy restoration from backups.

Responsiveness: Reducing the Duration of the Breach

How quickly organizations can recover from a cyberattack is facilitated by two interrelated principles: adaptation and embeddedness.

5. *Adaptation* is required to recover from known and unknown threats. All cyberattacks unfold in unpredictable ways, as the defender's and adversary's actions evolve in response to each other's moves. Recovering from a breach requires rapid learning cycles and ensuring that intelligence on the evolving situation is gathered, new actions are repeatedly tried, and successful measures are amplified.

In the first cyberattack by Russia on Ukraine's power grid, Russian adversaries took remote control of six grids' master control computers, locked out the Ukrainian operators, and shut down each neighborhood in five of the six grids one by one, turning off electricity to 250,000 households and businesses. The sixth grid stayed on due to the adaptive response of the operator. Realizing an adversary had taken control of his master computer, he pulled the Ethernet cable, disconnecting the computer and adversary from the grid. Although his response was not in the standard business continuity plan, the operator knew that the fail-safe condition of the grid was to continue supplying electricity to all customers.

6. *Embeddedness* embraces the principle that no system or organization is an island unto itself. An organization and its environment are part of an ecosystem of suppliers, employees, customers, competitors, and shareholders. When any individual organization is breached, it will impact many other constituents because they are interdependent.

Leaders are concerned about supply chain cyber vulnerabilities — and rightly so. The 2020 cyber breach via a SolarWinds software update infected at least nine government agencies and 18,000 companies, making the breach an ecosystem-wide issue. Similarly, malware inserted in a Kaseya software upgrade infected the point-of-sale systems of thousands of supermarkets and department stores, forcing many to close their doors. Cyber resilience requires having contingency plans for when any member of the ecosystem is compromised.

The broader ecosystem also has many resources to aid breached organizations. The cyber-resilient companies we studied have preexisting relationships with law enforcement, forensics experts, legal advisers, regulators, and communication experts. When hacked, they draw upon these existing relationships, which would take precious time to develop otherwise.

Shaping: After the Breach Is Over

This fourth time scale, which is often overlooked by organizations (as indicated by its mere 18% share of cybersecurity spending), is critical to how organizations learn from and prepare for future events. This is where reimagination comes in.

7. *Reimagination* is how resilient companies increase their future resilience within both the enterprise and the ecosystem after a breach.

Postmortem reviews that focus on lessons learned are often backward-looking, mechanical, technical exercises that provide only incremental improvements to incident response and business continuity plans. Cyber-resilient companies invest along two broader lines of thinking to maximize their performance for the future. First, they completely reimagine what else could go wrong and how they can better respond to known and newly imagined threats. Second, they use breaches as a stimulus to reimagine how to make overall enterprise operations and the extended business ecosystem more efficient and effective. This takes form by creating new alliances, norms, approaches, and models to address threats *and* opportunities.

One pharmaceutical company suffered an extended business interruption from a cyber event. After mitigating the cyberattack, the company was still unable to resume production because equipment was damaged beyond repair and replacement equipment was unavailable. Now, following the action principles in this article, the CEO requires all factories to regularly test their business continuity plans by practicing responses to scenarios such as, “System X has been disabled by a cyberattack, halting production. How do we get production running again?” Each factory is timed to see how quickly it can resume production. In addition, using the seven resilience principles, the pharma company has developed a number of new procedures and relationships, making it far more cyber resilient than before.

Because we often design organizations primarily to be successful and highly efficient, imagining all the possible things that could go wrong for an organization is very difficult, but the rewards are great. In the gym we say “no pain, no gain”; we stress our muscles, resulting in increased strength and resilience. Heart attacks prompt many people to eat healthier diets, exercise, and lose weight, thus realizing multiple benefits and becoming more resilient to heart disease and many other illnesses. In examining how they were able to continue operations under adverse circumstances, cyber-resilient companies like the ones discussed in this article discovered new ways to improve the overall effectiveness, efficiency, and performance of their enterprises.

To become a cyber-resilient organization, boards and management must shift their thinking from the current approach of 80% protection and 20% resilience to one focusing more on resilience.

Building a cyber-resistant organization is not just a blueprint for technology architecture but for the entire organization and its broader ecosystem. The companies we studied found the rewards worth the effort when they could confidently show their boards, customers, suppliers, and shareholders how their measured, managed, biologically inspired approach to cyber resilience gave them a competitive advantage over their peers and their cyber adversaries.

Topics

Managing Technology | Strategy | IT Governance & Leadership | Security & Privacy

ABOUT THE AUTHORS

Michael Coden is a senior adviser at BCG with over 30 years of experience in cybersecurity strategy. Martin Reeves (@martinkreeves) is a senior partner at Boston Consulting Group and chairman of the BCG Henderson Institute. Keri Pearlson is executive director of the research consortium Cybersecurity at MIT Sloan (CAMS). Stuart Madnick is the John Norris Maguire Professor of Information Technologies, Emeritus, at the MIT Sloan School of Management and the founding director of CAMS. Cheryl Berriman is global senior director of the CEO Advisory practice at BCG.

REFERENCES

1. The National Institute of Standards and Technology (NIST) Cybersecurity Framework has identified 98 subcategories: 25 related to identification, 35 related to protection, 18 to detection, 14 to response, and six to recovery.

2. These figures are based on BCG research that used data from Gartner, IDC, and NIST.

3. See the following sources, from which this concept of biological thinking and resilience came. Note that "time scales" refers to the time necessary for a given process or sequence of events. S.A. Levin, "Fragile Dominion: Complexity and the Commons" (Cambridge, Massachusetts: Helix Books, 1999); M. Reeves, L. Simon, and U. Daichi, "The Biology of Corporate Survival," Harvard Business Review 94, no. 1-2 (January-February 2016): 46-55; M. Reeves and J. Fuller, "The Imagination Machine: How to Spark New Ideas and Create Your Company's Future" (Boston: Harvard Business Review Press, 2021);

and Y. Sheffi, “The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage” (Cambridge, Massachusetts: MIT Press, 2005).

4. Least privilege access is a concept in computer security that limits users’ access rights to only what is strictly required to do their jobs. Zero trust is the concept that every user and every device must authenticate themselves when communicating with another user or device, to make it more difficult for an impostor user or impostor device to access systems in the enterprise. Network segmentation is the concept of putting different systems on smaller, individualized networks, with firewalls between the smaller networks to make it more difficult for an adversary to move laterally from one system to another.

TAGS:

Cybersecurity
Resilience
Risk Management
Strategic Planning

REPRINT #: 64301