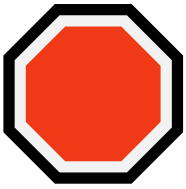
WILLIAM J. PERRY CENTER FOR HEMISPHERIC DEFENSE STUDIES

INSTRUCTIONS FOR THE ONLINE APPLICATION FORM

CYBER POLICY DEVELOPMENT
(CYBER 2022)

Application Period: 14 Jan – 28 Feb 2022

Preparatory Phase (Virtual): 13 Jun – 01 Jul 2022
Active Phase (Residential): 16 – 27 May 2022



WHO CAN USE THIS FORM TO APPLY

- Civilians (government and non-government)
- Retired military
- Non-military police
- Active duty military who live in the Washington, DC metropolitan area.

WE WILL NOT ACCEPT APPLICATIONS DIRECTLY FROM ACTIVE DUTY MILITARY PERSONNEL WHO LIVE OUTSIDE OF WASHINGTON, DC. THOSE INDIVIDUALS MUST CONTACT THE OFFICE OF MILITARY COOPERATION (MILGROUP) AT THE UNITED STATES EMBASSY IN THEIR COUNTRY TO APPLY.

For specific information, please contact our registrar's office at chdsregistrar@ndu.edu

---

Please follow all of the instructions on these pages, as well as those located online on our web page at **http://williamjperrycenter.org/academics**, which contains additional information not found on this here, including the Academic Integrity and Non-Attribution statement, which you agree to abide by if selected for the course.

Once you begin filling out the online application form, you will have to submit it in the same session. You will not be able to save your progress and return to it later.

The application process includes answering some essay questions, located on the online application form. The questions specific to this course are listed below in section 6. Before loading the application form, you might wish to review the essay questions and write your responses separately. The online application form will let you copy and paste text into the appropriate text boxes.

The application form is located at the following URL:

https://www.dscarc.org/default?regcenterid=11&eventid=58171&reltype=12479

Please keep in mind that the Perry Center shares this application system with other regional centers; therefore the form is initially presented to you in English. In the upper left-hand side of the page, there is a drop-down menu for automatic translation into various languages. This is designed to help you better understand the application form, but please keep in mind that machine translation is not perfect.

4

After you complete the online application form and have received your confirmation number, please send the following documents to **chdsregistrar@ndu.edu**:

- **Two (2) letters of recommendation:**
  - One of the letters must be from your supervisor / chain of command.
  - Both letters should specifically indicate what you would be contributing to the course, and what benefits you and/or your organization would derive from your attendance, should you be selected to participate.
  - Both letters must be dated no earlier than 60 days before your actual application date.
  - Individuals who are independent contractors or sole proprietors must still submit two letters of recommendation from professional references addressing the above points.
  - Both letters should be addressed to the Director of the William J. Perry Center for Hemispheric Defense Studies.
- **Professional Experience Form (available for download directly below). The form must be completed fully. DO NOT ATTACH a copy of your own CV in lieu of completing the form:**
  - English version - **https://bit.ly/ExperienceForm-EN**
  - Spanish version - **https://bit.ly/ExperienceForm-SP**

When you send your documents via e-mail, the subject line must contain your last name, country, course, and confirmation code provided to you by the system. *Failure to provide this information with your documentation may result in delays processing your application.* Example: **SMITH – JAMAICA – CYBER 2022 – QPLFHNJ1234**.

Please ensure that the combined total file size of your attachments does not exceed 8 MB. We will not grant deadline extensions due to messages being rejected by our e-mail server. **Applications will not be considered complete until the Perry Center receives all of the required documents (Online application form, Letters of Recommendation, Professional Experience Form)**

5

Upon submitting an application, you certify that you:

- Have read the general course description, candidate profile, and the application instructions on this document and web site.
- Understand that this includes a two-week preparatory phase before the active phase begins. You will actively participate in all the online sessions and promptly complete assigned homework. Successful completion of the preparatory phase is required to attend the active portion of this course.
- Understand these instructions and agree to abide by the National Defense University's Academic Integrity Policy.
- Understand that all courses are subject to availability of funds.
- Meet the language requirements for this course.
- All information you have provided is accurate and truthful.

All applicants will receive notification via e-mail approximately three weeks before the start of the preparatory phase if they have 1) been selected, 2) have been placed on the waiting list, or 3) have not been selected.

6

ESSAY QUESTIONS

1. Please describe in detail your current job duties and work activities in relation to cybersecurity at the policy and strategic level. (200 word max)

2. Please describe how this course will help you personally (now or in the future), or your organization, to develop a policy (and/or strategy) for cybersecurity. (200 word max)

3. After reading the included article, what is your opinion of its application in cybersecurity at the policy and strategy level? (300 word max)

Make Cybersecurity a Strategic Asset

By elevating cybersecurity from an operational necessity to a source of opportunity, leaders can boost resilience and business advantage.

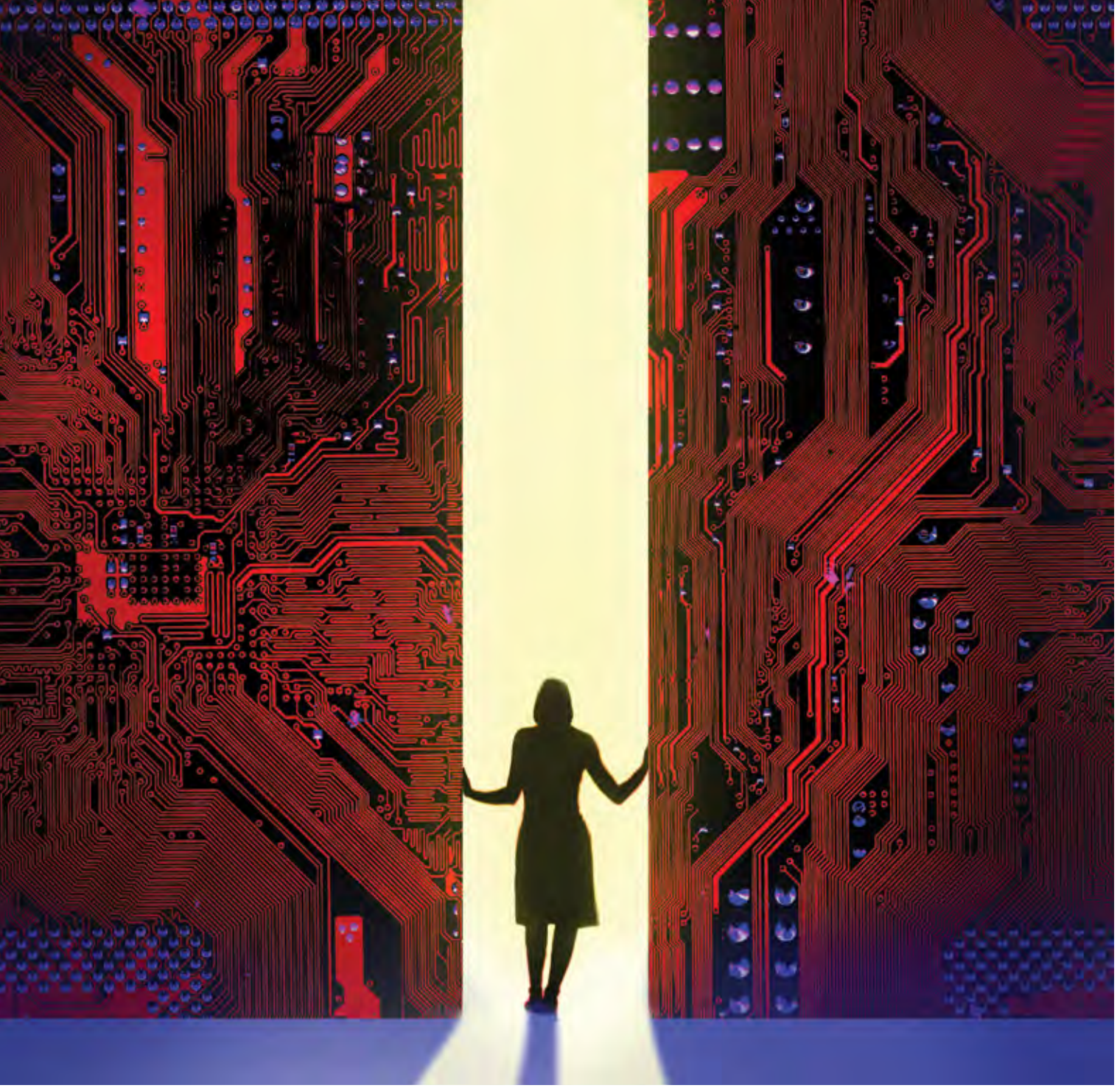
BY MANUEL HEPFER AND THOMAS C. POWELL

On June 27, 2017, employees in more than 80 global companies booted up their computers only to find a black screen with the message, "Oops, your important files are encrypted," along with a demand for a bitcoin payment to decrypt the files. Within a few hours, managers began to realize the extent of the attack: Malware had infected the companies' central servers, paralyzing every aspect of global operations, including interoffice communications, access to documents, access to customer data, and all operational and manufacturing systems. The NotPetya virus, which had begun its spread via the software-update function of a widely used Ukrainian tax preparation program, eventually caused global economic damage exceeding $10 billion in industries such as transportation, energy, pharmaceuticals, food production, consumer goods, and professional services.[1]

Despite such examples of devastating cyberattacks on major organizations, many of the world's largest companies remain unprepared.[2] Although executives acknowledge cybersecurity as an important part of IT planning, they misunderstand the strategic character of cyberattacks, both as a severe threat to earnings and operations, and as an opportunity. Yes, an opportunity.

We studied three global companies, competing in logistics, consumer goods, and professional services, that suffered from the 2017 NotPetya attack.[3] (See "The Research," p. 42.) We found that executives who have successfully managed through cyberattacks now recognize cybersecurity as a top-level strategic priority; they told us that their biggest mistake in the period before the NotPetya attack was to treat cybersecurity as an operational issue. Having experienced an attack, executives at the consumer products company recognized that cyberattacks can't be prevented but must be prepared for, while the board realized that an attack's impact is not limited to IT but rather affects the viability of the whole business.

What these executives came to understand is that organizational resilience to cyberattacks requires a



fundamental change of mindset: Executives must view cybersecurity as *strategic* rather than operational, and as an *opportunity* rather than an expense.

What do we mean by "opportunity"? A mature cybersecurity strategy provides a basis for securing critical assets and business processes, enhancing organizational learning, and noticing and capturing new strategic opportunities. It can reveal new strengths and fundamental weaknesses in leadership teams and organizational capabilities. Among the companies we researched, some found that it paved the way to a fully digital business model or helped them create a new value proposition around security for customers. Our research offers new ways of thinking about cybersecurity and provides a simple framework for assessing organizational resilience.

Why Executives Treat Cybersecurity as Operational, Not Strategic

It is easy to understand why executives fail to recognize cybersecurity as a strategic priority, even as many have embarked on digital transformation strategies.

Cybersecurity is delegated to IT. Maintaining secure systems has traditionally been the responsibility

GARY WATERS/THEISPOT.COM

THE RESEARCH

We studied three global companies — in logistics, consumer goods, and professional services — that suffered from the 2017 ransomware attack known as NotPetya. We interviewed their CEOs, CFOs, CIOs, and other senior executives and reviewed internal documents, presentations, and audio and video files related to events before, during, and after the cyberattack.

We interviewed other industry participants and cross-checked our findings with executives in companies that had experienced different cyberattacks and with experts in cybersecurity consulting, cyber-insurance, forensic services, and information security.

Based on our interviews and data, we prepared comparative case studies of cyberattack preparation, response, and resilience and developed the concepts described in this paper.

of IT — and, in many cases, IT itself is not seen as a provider of strategic advantage but rather as an internal service provider primarily accountable for keeping systems running. Even as the cyberthreat to business has magnified dramatically, and as technology has in many cases been recognized as more strategic to the business, cybersecurity has remained delegated to IT operations, where the technical expertise necessary to assess and respond to cyberthreats resides.

Companies misunderstand the strategic nature of cybersecurity risk. Many executives fail to elevate the risk of cyberattack to a strategic consideration because they mischaracterize the threat as a random, unpredictable event — when, in fact, no organization is immune, and cyberattacks are "predictable surprises" that exploit weaknesses in organizational strategies and capabilities. Some companies are more attractive targets than others, but in reality, cybercriminals directly attack organizations of all kinds, and many other businesses suffer collateral damage in the course of attacks on other companies.

Companies keep attacks under wraps. One CEO in our study reported having some processes and measures in place, but once his company was victimized, it quickly realized how ill-prepared it was and how little it actually knew about the real risks of being hit by an attack. Such naivete may be exacerbated by the tendency among organizations that have suffered an attack to release as little public information about the event as possible — which may serve to downplay the true extent of the risk. Keeping cyberattacks confidential also means that best practices for responding to them are not shared and executives cannot learn from cyberattacks on other companies.

Executives assign strategic priorities based on their own areas of expertise. We also found that executives have failed to include cybersecurity among their strategic priorities because their strategic plans and major investment decisions have focused on areas in which they had previous experience or technical expertise, such as engineering, finance, and marketing. Cyberattacks are nonroutine and hard to plan for, and many executives have not experienced a serious cyberattack. The cognitive tendency is to carry on with the same strategic priorities, interpreting the absence of a cyberattack as evidence that the company is on the right track. After the NotPetya cyberattack, executives understood the importance of defining strategic issues according to their potential impacts on company performance.

Flipping the Narrative on Cybersecurity

Senior executives who guided their companies through cyberattacks experienced a fundamental change of mindset, transforming their perceptions of cybersecurity from operational to strategic, from reactive to proactive, and from threat-driven to opportunity-driven. In practice, this meant taking cyberthreats seriously at the highest levels of decision-making. The CEO of a logistics company told us, "Prior to the attack, I had never envisioned that a cyberattack could go global in an instant, which was really a huge surprise. We were doing something about cyber, so it looks like we are doing something [right], but it was much more of a tick-the-box exercise instead of really understanding it."

Before the NotPetya attack, executives made the mistake of viewing cybersecurity investments as a lose-lose situation. They felt that if their company was attacked, they would lose reputation and profit; if their company was not attacked, investments in cybersecurity would be wasted. As a result, the companies had underinvested in cybersecurity.

Following the cyberattack, executives appreciated the strategic value of investments in cybersecurity, not only for mitigating risk or minimizing damage but for strengthening the core strategic capabilities of the company. For example, a professional services executive told us that the cyberattack "was an existential threat to our business, and one of the things it shows is where you have strong leadership and weak leadership." As crises tend to do, the attack explicitly highlighted those pockets of weakness; had the company taken a strategic approach to preparation, it would have known which leaders needed better training to handle the response.

In the logistics business, where competitiveness depends on speed in bringing new solutions to market, cybersecurity investments transformed the company's competitive position by driving it to standardize digital solutions across its operations. Executives learned from the NotPetya attack that the company was not a purely physical business but a data-intensive digital business. The new technology

infrastructure allowed the company to implement a fully digital business model; it rolled out a new transport management solution in just nine months from start to finish. According to a company executive, "Our biggest competitor did the same and it is taking them seven years, and the main reason for this is our standardization today."

How Cybersecurity Strategy Reveals Opportunity

Our research shows that executives can leverage cybersecurity strategy to enhance organizational learning and create new opportunities. Companies that suffer cyberattacks find that an attack exposes weaknesses not only in cybersecurity but in many other aspects of the business, such as leadership development, external communications, and process innovation. Accordingly, the process of developing a comprehensive cybersecurity strategy, as outlined later in this article, can similarly uncover weaknesses and opportunities.

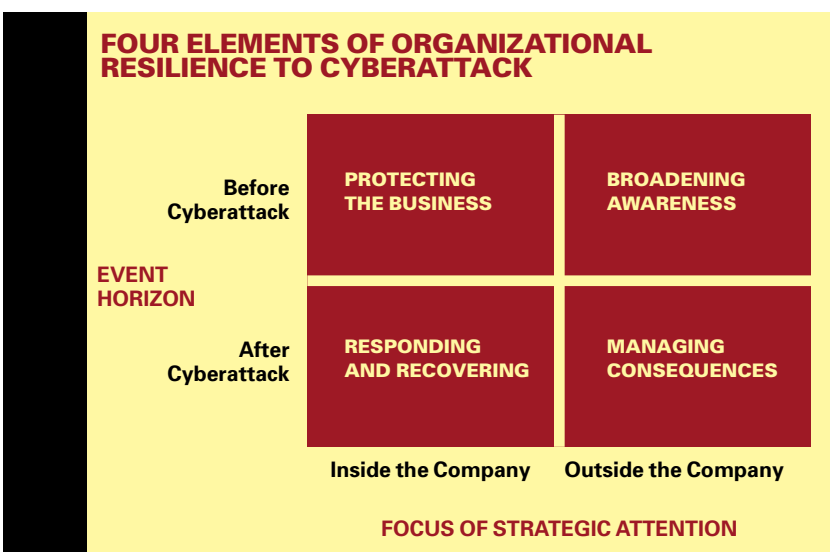
Before the attack, executives at the logistics company thought that its most critical process was moving cargo, but subsequently they realized that the most critical process was bookings — and thus they reconfigured their strategic priorities. In implementing a new, robust cybersecurity strategy in the wake of the attack, the company identified its seven most critical business processes. Diagramming the interconnectedness of these critical processes helped executives discover how the NotPetya virus had spread so quickly through the enterprise and why it took so long to recover servers and applications. In essence, the company changed from protecting its IT infrastructure to protecting its most critical business processes.

By disabling core business processes, the NotPetya attack exposed organizational weaknesses that were previously unnoticed or ignored. In some cases, the crisis prompted improvisational solutions that might have taken years to discover. For example, a logistics executive told us, "During the attack, the hierarchy of the organization completely broke down. There was no hierarchy at all. We assembled hierarchy and structure dynamically as we needed to. What might normally take two years to change, we were changing within 18 hours. We selected people based on skill, knowledge, and their ability to lead certain aspects. Suddenly we had four directors reporting to someone from the very bottom of the organizational chart. In one example, we promoted someone four times after the cyberattack."

Gaining a more strategic understanding of cybersecurity creates the opportunity for closer integration and understanding between business and IT. "The cyberattack made us understand that IT is cutting across the whole business," one executive in consumer goods told us. It revealed to people in areas as varied as supply chain and HR how IT underpins even the most basic business activities, such as printing a label for a box or tracking hours worked and paying wages, he said.

Capturing Strategic Opportunities From Cybersecurity

From our research, we have developed a model for evaluating and improving organizational resilience to cyberattacks and for leveraging cybersecurity strategy to achieve new forms of advantage. The model (see "Four Elements of Organizational Resilience to Cyberattack") shows that organizational resilience requires four strategic capabilities: protecting the business, broadening awareness, managing consequences, and responding and recovering. Each of the four elements raises questions that executives can use to lead discussions on the company's approach to cybersecurity strategy. Although some of these discussions are concerned with events after a cyberattack, all of the discussions should happen now, as part of strategic planning — *before* a cyberattack.



Protecting the business, especially the IT infrastructure, has traditionally accounted for the lion's share of cybersecurity spending. While it remains important to maintain and harden defenses, companies in our study acknowledged that attacks are nonetheless inevitable. The war between cybercriminals and cybersecurity experts is an arms race of sorts, with both attack vectors and defenses continually evolving, rendering perfect defense impossible. The companies we studied advised that first-level protection should not entirely consume cybersecurity budgets or efforts. One CEO told us, "What we realized is that the protection we had was a hard shell. But once you penetrate that hard shell, we were completely soft inside." A more strategic approach to protection is layered and encompasses a deeper understanding of key business processes and how they might be designed to minimize an organization's vulnerability to attacks.

Your strategic planning for protecting against an attack should consider these questions:

- What are our key business processes?
- How vulnerable are they to cyberattacks?
- What are we doing to protect ourselves?
- How can we design our business processes to minimize our vulnerability to attack?
- What internal capabilities do we have for protecting against cyberattacks?
- Where are the strategic opportunities for improving cyber-protection?

Broadening awareness requires senior management to take responsibility for looking outside the company to understand current threats and to develop a more comprehensive strategy for acquiring intelligence. These actions include establishing better connections into the network of threat intelligence, such as communicating with cybersecurity researchers at anti-malware vendors and building relationships with peers at organizations with the strongest capabilities in this area. In our interviews, a board chair recommended retaining and consulting with an expert cyber-response adviser before there's a crisis, and a CEO advised having an outside organization regularly perform security audits.

To develop a fuller awareness of the threat landscape, ask these questions:

- How significant is the threat of cyberattack?
- Where is it most likely to come from?
- What form might it take?
- How are cyberattacks evolving?
- What capabilities do we have for detecting external threats?
- Where are the strategic opportunities for improving cyber-awareness?

Managing the consequences of an attack, like broadening awareness, demands that leaders look outward to plan for the potential effects of a cyberattack on customers, suppliers, financial markets, and the company's reputation. The companies in our study suggest being open with information, as well as open to help — essentially, doing what many companies hesitate to do. The decision to communicate openly with customers, shareholders, and the general public proved especially valuable, according to a CEO in our study. It generated not only positive customer feedback but also numerous offers of help from customers, suppliers, and even competitors. For example, a professional services business built new relationships with competitors that offered their computing facilities and office space in the wake of an attack. And communicating proactively with your biggest customers reassures them about your cybersecurity practices while providing a potential source of competitive advantage: A logistics executive told us that after the company had been accredited to a security standard, it had won two significant pieces of business.

Develop a strategy to manage the external consequences of a cyberattack by considering the following:

- How would our key stakeholders respond if we were attacked?
- How would our customers be affected?
- How would financial markets respond?
- What can we do now to anticipate or shape these responses?
- What capabilities do we have for anticipating how stakeholders might respond?
- What are the strategic opportunities for managing the consequences of a cyberattack?

Responding and recovering requires understanding the organization's capabilities to take appropriate action in case of a cyberattack and identifying

potential weaknesses in processes, leadership skills, and backup plans. Executives in our study advised that response should focus first on recovery and spoke to the importance of having top leadership support for technology teams throughout the recovery effort. It is also essential to consider the composition and leadership of response teams: The head of operations for one company said that in the aftermath of a cyberattack, it continuously broke down and reassembled teams and changed team leaders based on who emerged as the strongest people for those roles. Plans for a cyberattack response should always include spotting opportunities — as the saying goes, "When the barn burns down, you can build a better barn." In the aftermath of a cyberattack, managers must proactively seek new ways to position IT as a value generator rather than a cost center and leverage events to strengthen the company's strategic position.

These questions should guide your plan for a robust response and recovery in case of attack:

- What capabilities do we have for responding to a cyberattack? What weaknesses would hinder our responsiveness?
- What can we do now to improve our responsiveness to an attack?
- What is our plan for business continuity in case of a cyberattack?
- How do we build an organizational structure that is dynamic enough to respond to different types of attacks?
- Who should be part of our crisis management team?
- What new strategic opportunities might be created if we improved our capabilities for cyber-responsiveness?

PROACTIVELY ADDRESSING EACH of these four elements of organizational resilience to cyberattacks, and considering each set of questions above in the planning process, allows executives to identify strategic opportunities that arise in all phases of the cybersecurity context and develop critical capabilities *before* a cyberattack happens. A crucial finding in our study is that resilience to cyberattacks requires advanced capabilities in *all four elements* of the model.

The companies in our study that suffered the greatest long-term damage from the NotPetya cyberattack — competitively, economically, and reputationally — were those that neglected one or more elements of the model. By far, the most common error was to focus on protection while neglecting the other elements. Every company had made prior investments to protect against cyberattacks and (to a lesser extent) to plan cyber-responses. These investments were largely wasted, however, because leaders considered the threats as having consequences only within their IT departments rather than potentially paralyzing the entire business. After a cyberattack, all of the companies expanded their cybersecurity strategies by significantly increasing investments in broadening awareness and managing the consequences of a cyberattack.

Our research shows that companies can improve resilience to cyberattacks by interrogating each of the four elements of organizational resilience as part of the company's strategic planning process. The evidence shows that asking these questions now, before a cyberattack, allows companies to work proactively toward capturing new opportunities afforded by the context of cybersecurity strategy. By adopting a strategic mindset toward cybersecurity, executives can leverage cybersecurity strategy to enhance organizational resilience and to build new capabilities for strategic advantage.

Manuel Hepfer *is a doctoral student at Saïd Business School at the University of Oxford.* ***Thomas C. Powell*** *is a professor of strategy at Saïd Business School.*
Comment on this article at https://sloanreview.mit.edu/x/62120.

REFERENCES

1. A. Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired, Aug. 22, 2018, www.wired.com.

2. See, for example, P. Mee and J. Cummings, "Is Your Company Ready for a Cyberattack?" MIT Sloan Management Review, Dec. 4, 2018, https://sloanreview.mit.edu; R.A. Rothrock, J. Kaplan, and F. Van der Oord, "The Board's Role in Managing Cybersecurity Risks," MIT Sloan Management Review 59, no. 2 (winter 2018): 12-15; and M.E. Mangelsdorf, "What Executives Get Wrong About Cybersecurity," MIT Sloan Management Review 58, no. 2 (winter 2017): 22-24.

3. To preserve confidentiality, we are referring to the companies by industry — logistics, consumer products, and professional services — rather than by name.

Reprint 62120.