bcg.perspectives
by THE BOSTON CONSULTING GROUP

BUILDING A CYBERRESILIENT ORGANIZATION

By Stefan A. Deutscher, Walter Bohmayr, and Alex Asen

Despite steadily mounting evidence to the contrary, many executives seem to imagine that, in the realm of cybersecurity, a robust defense is all their company needs. But those executives may experience a rude awakening. No defense, no matter how well constructed and maintained, is 100% impenetrable. Computer systems are subject to compromise. Data, including both sensitive company information and information about customers and clients, is vulnerable to theft or tampering.

The upshot: companies can't afford to focus their security efforts solely on their ability to ward off attacks and expect this strategy to fully protect them. Instead, they must ramp up their organization's *resilience*—its ability to continue to function after the company suffers a breach (as it almost inevitably will) and to recover gracefully after even a serious security lapse.

Building organizational cyberresilience entails understanding the three phases of a successful attack: the before, the during, and the after. How well your company—meaning both its own people and external parties and partners such as temporary staff and contractors—grasps and is prepared for each phase can make an enormous difference in whether a breach proves relatively innocuous or takes a massive toll on your business. (See the sidebar "Getting the People Part Right.")

Before an Attack

The period before an attack can last as long as the attacker chooses. During this phase, the attacker scouts its prey (your company) to understand its technical defenses and identify its vulnerabilities. For defenders, this is the time to take three critical steps.

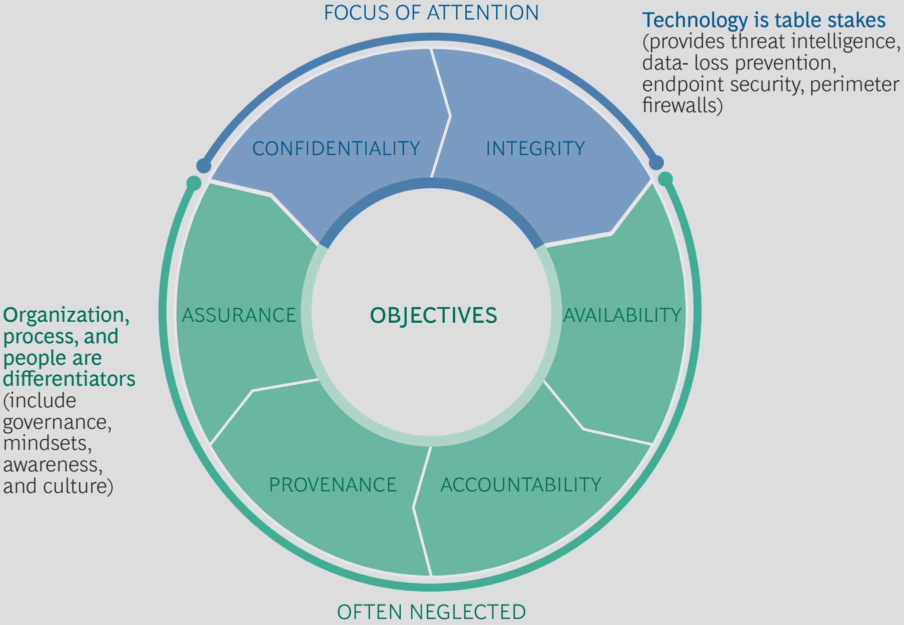
Create awareness among both IT and nontechnical staff of the potential for cyberattacks. Simple yet powerful ways to raise awareness include distributing mail and video messages from top management; reporting attacks or incidents on the company's intranet site(s); and—emulating a best practice of businesses in the mining, construction, and engineering industries—

GETTING THE PEOPLE PART RIGHT

A full treatment of corporate cybersecurity would span a number of topics not addressed in this article, including governance and processes. We have chosen to focus primarily on one element: the people side.

Why? Because cybersecurity starts with people. Many companies pay lip service to the importance of a holistic "people-process-technology" approach to cybersecurity. But in our experience, they tend to focus primarily on technology, while neglecting issues of organization, process, and people. (See Exhibit 1.) This can be a costly mistake, because the importance and vulnerability of people, in particular, cannot be overstated.

EXHIBIT 1 | Companies Focus Too Much on Technology and Too Little on Organization, Process, and People


FOCUS OF ATTENTION
Technology is table stakes
(provides threat intelligence, data- loss prevention, endpoint security, perimeter firewalls)
CONFIDENTIALITY
INTEGRITY
ASSURANCE
OBJECTIVES
AVAILABILITY
PROVENANCE
ACCOUNTABILITY
Organization, process, and people are differentiators
(include governance, mindsets, awareness, and culture)
OFTEN NEGLECTED

Source: BCG analysis.

making "safety moments" a mandatory part of every company meeting.

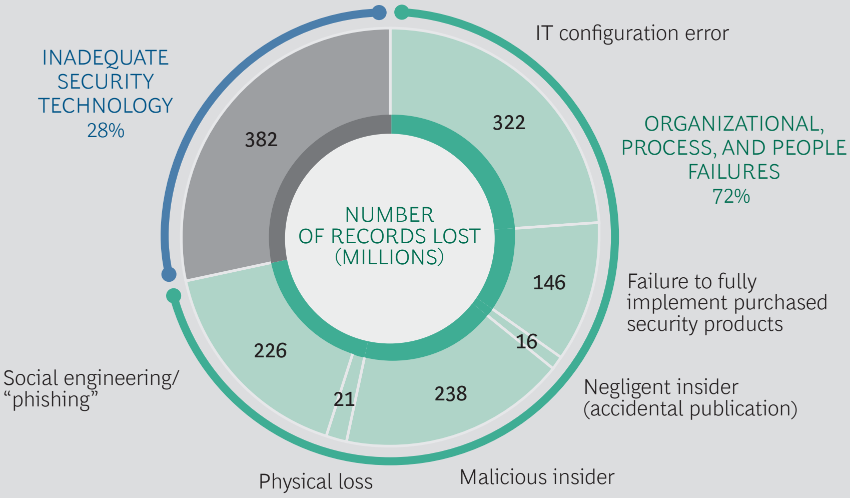
The company should supplement its ongoing awareness campaign with appropriate training. It is critical that your IT staff be able to recognize early signs of an attack, distinguish an attack from unexpected but legitimate behavior on the part of the company's IT systems, and react effectively. You should strive to create a culture that tolerates false positives—IT staff should not have to worry about crying wolf too often. You should also ensure that nontechnical staff understands the importance of being prudent—for example, not clicking on unexpected e-mail attachments. Such prudence is vital, as today's cyberattackers are both aggressive and devious. Over the past couple of years, for example, attackers have increasingly targeted senior executives' assistants with "spear phishing" attacks (which rely on individualized, often highly tailored e-mail messages spiked with malicious attachments). A successful attack of this type can be as valuable to the attacker as one that gains direct access to the accounts of senior executives themselves, since many executive assistants have full access or far-reaching delegate rights to

GETTING THE PEOPLE PART RIGHT
(continued)

A company's people are crucial to establishing a successful cybersecurity program and building the resilience needed to bounce back from a breach. They will be at the forefront of designing, testing, implementing, and operating your defenses. If your people are smart, committed, well trained, and prepared, they will be your strongest bulwark against a truly damaging attack. Conversely, their failures, whether due to malicious intent, negligence, or ignorance, will likely be the source of your next breach. Indeed, a review of 50 of the largest recent data breaches reported worldwide between May 2011 and May 2016 reveals that a relatively small proportion of records lost as a result of those breaches stemmed from inadequate security technology. Most losses are attributable to failures involving organization, process, and people. (See Exhibit 2.)

Exhibit 2 | Organizational, Process, and People Failures Are the Main Source of Critical Breaches

CAUSES OF DATA LOSSES IN 50 MAJOR BREACHES



Sources: Press reports; company statements; BCG analysis.
Note: Of the more than 1.8 billion records lost in these 50 data breaches, 490 million were excluded from our analysis because there was insufficient information to determine a root cause.

their bosses' mailboxes, calendars, documents, and contacts (which can be helpful to an attacker seeking to build the next step in a targeted attack).

The company should also stress the importance of such prudence to technical staff, whom attackers often target with similar tactical assaults. Administrators of pivotal IT systems (such as central infrastructure services, essential business systems, and the company's communications infrastructure) are especially popular targets of carefully designed social engineering attacks, as well as of attacks on their private personal computers by outsiders seeking entry into the company's systems.

Employees throughout the organization should receive tailored training—and the training effort should start at the very top, with the organization's C-suite, board of directors, and even supervisory boards.[1] Those individuals can benefit tremendously from awareness and enablement sessions, tabletop simulation exercises, and full-fledged war-gaming sessions.[2] For technical people, the training should include special skills training—for example, lessons in how to harden systems, detect systems that do not conform to policies, and write realistic policies. For general staff, social-engineering awareness training can be very useful, especially when combined with real-life testing (using company-commissioned fake phishing e-mail messages, for example).

Think carefully about the design, implementation, and configuration of your company's technology system—especially access rights. Ensure that it covers the basics. Confirm that your technical staff has configured IT systems securely and has hardened them against attack to the extent possible.

Aim for a reasonable role-based access management system for nontechnical staff—one that keeps people separated from applications or data they don't need. (The use of expiration periods to limit access for people in specific roles is one effective way to restrain "privilege creep.") The same approach should apply to IT employees, confining their reach to systems that they need unfettered access to, ensuring that they do not claim higher-than-necessary privileges (for example, system administrator rights) for routine tasks, and enforcing appropriate logging for activities that do require higher privileges.

It may help to look at the practices of government entities, which commonly vet employees and assign them different security and access classifications, with different levels of permission to use certain systems. Such fine-grained control may not be economically feasible for all organizations, but studying approaches that involve this degree of sophistication can provide valuable insight into how a company might establish roles and rights in a simpler security design.

Plan for during and after while you still can. In the period before an attack, companies can act under their own control. But when a serious attack is underway, they may be reduced to reacting or, in a worst-case scenario, simply watching as the attack unfolds. Operators of the Ukrainian power grid found themselves in precisely this state when attackers hacked the grid in December 2015.[3]

Beforehand, companies can focus on taking steps to prepare for an attack and its aftermath. These measures include what we call the "cybersecurity 101s," which include identifying the company's most valuable assets, identifying risks, defining protection objectives, and instituting appropriate risk-management approaches. (See "Cybersecurity Meets IT Risk Management: A Corporate Immune and Defense System," BCG article, September 2014.) Other actions that companies can take include the following:

- Identify external parties that the company will need to engage in the event of an attack or breach, and determine how to reach them. At the same time, gauge the extent to which an internal security function can provide the desired capabilities for protection, detection, and response, and whether sourcing all or part of that function might be a viable alternative.

- Write, implement, and test emergency operations, business continuity measures, and disaster recovery plans.

- Run tests and establish a testing regimen to ensure continual reassessment of the company's degree of readiness. Such testing might include tabletop simulation exercises for senior management (for example, "What would we do if our manufacturing operations in Asia were brought down by a cyberattack?") and penetration tests performed by "ethical hackers" whom the company pays to relentlessly probe and detect weaknesses in the company's defenses.

- Determine how the organization can ensure reliable, trustworthy governance during a breach, when elements of systems—including key communications such as e-mail and IP-based telephony—

may be compromised or operators locked out of their systems altogether, as happened to the Ukraine grid operators when cyberattackers breached their system. (Companies may face even more-serious threats during a cyberattack. During the highly publicized Carbanak attack of 2015, which targeted a large number of banks and reportedly resulted in an aggregate loss of about $1 billion, attackers could read company communications, view company videoconferences, and watch employees through their laptop cameras.)

- Create and test communications policies and plans (such as who is authorized to say what during an attack) so that the company's dissemination of information stays ahead of media coverage.
- Make sure that everyone assigned a role in emergency plans is aware of and accepts that role. In our casework, we have found instances where named response managers had never heard of the company's emergency plan or had long since left the company. Also, make sure that every individual assigned a role has an identified backup—not just during the regular work week, but on weekends, public holidays, and individuals' vacation days.

During an Attack

Often a company fails to recognize initially (or at all, in some instances) that an attack is unfolding—even though it has developed strong internal technical and human defense capabilities or engaged specialized companies to provide monitoring and detection services. If and when your company sees that it is under siege, there are several important things it can do in response.

Mobilize in a controlled way. Kick off a (prepared and practiced) standard response process. If a severe attack or breach occurs, mobilize a core response team.

Communicate to the organization that an attack is underway and that teamwork is essential. A serious attack will impose extraordinary demands on the company and its people. Providing transparency and focusing on solutions rather than on finger-pointing is important: the company and its components (organizational units, legal entities, and functions), including IT, the cybersecurity unit, HR, risk management, communications, and the business lines, must mobilize quickly and work together as a well-oiled, flexible unit to defend itself. During this period, decisions about external communication—especially on the question of how much detail to divulge—should take into account both legal concerns about revealing too much information and the potential harm to the company's brand of failing to share critical information with customers and other stakeholders in a timely manner.

Thoroughly address serious attacks, detected breaches, and loopholes as they arise. The company's various units will have to work hand in hand to ensure that people immediately report detected breaches and security loopholes to the appropriate internal parties, who must then act swiftly to mitigate the damage (or at a minimum, gain a fuller understanding of what the attack has done or is doing). Throughout the crisis, the company must also ensure that it actively manages communications with internal and external stakeholders—including employees, senior management, customers, the media, and regulators—and that it continues to meet its regulatory-reporting duties and deadlines.

Leverage external resources as necessary. Even the best-prepared organizations can find themselves overmatched during an attack. In such cases, the company should "call in the troops," which might include specialized private-sector companies and public law enforcement, as needed. The company's ability to quickly access these resources rests on pre-established contracts with the necessary parties, appropriate and well-documented processes for invoking their support, and people within the company who are authorized to kick the process into gear. Playbooks developed for the "before" period should address and document all of these needs.

"AFTER" IS IN THE EYE OF THE BEHOLDER

The period after an attack can mean different things to different people. For a defender, the connotation is straightforward: the immediate assault has ended, and the time to repair and regroup begins. For an attacker, however, "after" may refer to the period between the piercing of the defender's hull and the point at which the target company detects and closes the breach. Attackers use this period to exfiltrate information or to install additional malicious payload (so-called back doors or even more-advanced threats that, like sleeper cells, lie dormant and evade detection until activated from the outside). In some instances, attackers may simply wait through much of the period between breach and detection before pulling the trigger on the poison they introduced through the breach.

In other words, sometimes the worst of the damage occurs in the "after" period. The case of Nortel (now defunct) makes this amply evident. The company believed that the attack was over, but it was actually in the middle of a breach that lasted for about ten years, in the course of which hackers had ready access to company communications and intellectual property.

After an Attack

Once the dust has settled, the company needs to ensure that it will not fall victim to the same attack a second time. (See the sidebar "'After' Is in the Eye of the Beholder.") Companies can do four things to maximize their chances of success in this effort.

Work across functions and units to understand the attack and ensure that staff has plugged the holes and updated defenses and processes. An analysis that strengthens the company's defenses and yields significant lessons is much easier to conduct in an open environment, in which employees are unafraid to speak up. To foster this type of environment, organizations should institute a "blameless" postmortem culture. Such a culture has been highly effective following accidents and near-misses in the aviation industry, for example, and can facilitate learning in the aftermath of a corporate cyberbreach as well. If a culture of this type is difficult to create within the organization in a given time frame, the company should, at a minimum, establish a channel for anonymous whistleblowing—one that serves a function similar to that of an ombudsperson.

Identify employees who can collaborate with internal and external experts on security-related issues, and establish dedicated roles for them within the company. The company may need to consult forensic companies, communication firms, training firms, auditors, legal advisors, the media, and law enforcement personnel. Once you have identified employees who can collaborate effectively with such experts, give them the latitude to concentrate on this role as necessary. Doing so may entail temporarily relieving them of their standard duties and changing reporting lines. It may also require the creation of new, dedicated positions staffed with appropriate personnel (in terms of skills and numbers).

Inform everyone affected by the attack or involved in the defense effort—including internal and external parties—that things are back to normal. This announcement will help everyone achieve closure. Here, as elsewhere, the communications department should take the lead in the company's communications efforts—but the entire organization, from top to bottom, needs to be able to communicate effectively and consistently on this front. This is also a good opportunity to thank those involved in the defense and recovery efforts (including corporate teams, individuals, and external partners, to the extent that they can be named), either before a broader audience or privately. (Not all cyberheroes will want to be publicly exposed).

Remain vigilant. After the organization has returned to normal following a breach, it is important to combat complacency. Be sure to see the root-cause analysis of the breach through to its resolution and to incorporate the knowledge gained from the experience into the company's processes, knowledge management systems, technical landscape, testing scenarios, and organizational setup.

Things to Do Monday Morning

If you are concerned about your company's ability to weather an attack or a breach, where should you focus your attention first? The following steps are very important:

- If you are starting fresh and have no data on attacks or breaches suffered by your company, review and begin to undertake the activities described above in the section "Before an Attack." If you do have such data, try to supplement it with additional threat intelligence for your industry or company. (In many instances, you can obtain this type of information from membership-based organizations and professional security services firms.)

- Run a cybersecurity health check that assesses not only the security controls that the company has in place but also the capability maturity of your organization and its processes. (See "Getting Fit for Transformation: The Other Technology Strategy Every IT Leader Needs," BCG article, July 2015.)

- Perform a training session on C-suite enablement, possibly in association with a tabletop simulation or a more detailed war-gaming exercise.

- Confirm that your company's training and corporate communications agenda includes cybersecurity-related offerings. In addition, confirm that your corporate communications department has cybersecurity-related scripts for external and internal use.

- Check that your company has developed up-to-date response plans, and verify the details of your company's contracts with outside support on call.

- Start to build a cybersecurity management system, or launch a review of your existing one.

Notes

[1] See "Why should we care about cyber resilience? Because $445 billion is at stake," World Economic Forum, September 8, 2016, https://www.weforum.org/agenda/2016/09/why-should-we-care-about-cyber-resilience-because-445-billion-is-at-stake.

[2] See "How to prepare for the cyberattack that is coming to your company," World Economic Forum, November 30, 2016, https://www.weforum.org/agenda/2016/11/how-to-prepare-for-the-cyberattack-that-is-coming-to-your-company.

[3] See "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired,* March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

About the Authors

Stefan A. Deutscher is an associate director in the Berlin office of The Boston Consulting Group and a core member of the Technology Advantage and the Technology, Media & Telecommunications practices. He is BCG's global topic leader for cybersecurity and IT risk management as well as for IT infrastructure and data center operations. You may contact him by e-mail at deutscher.stefan@bcg.com.

Walter Bohmayr is a senior partner and managing director in the firm's Vienna office and a member of the Technology Advantage, Energy, Financial Institutions, and Technology, Media & Telecommunications practices. He is BCG's global leader for cybersecurity and IT risk management. You may contact him by e-mail at bohmayr.walter@bcg.com.

Alex Asen is a senior knowledge analyst in BCG's Boston office. He is a core member of the firm's Technology Advantage practice and a member of the global cybersecurity leadership team. You may contact him by e-mail at asen.alex@bcg.com.