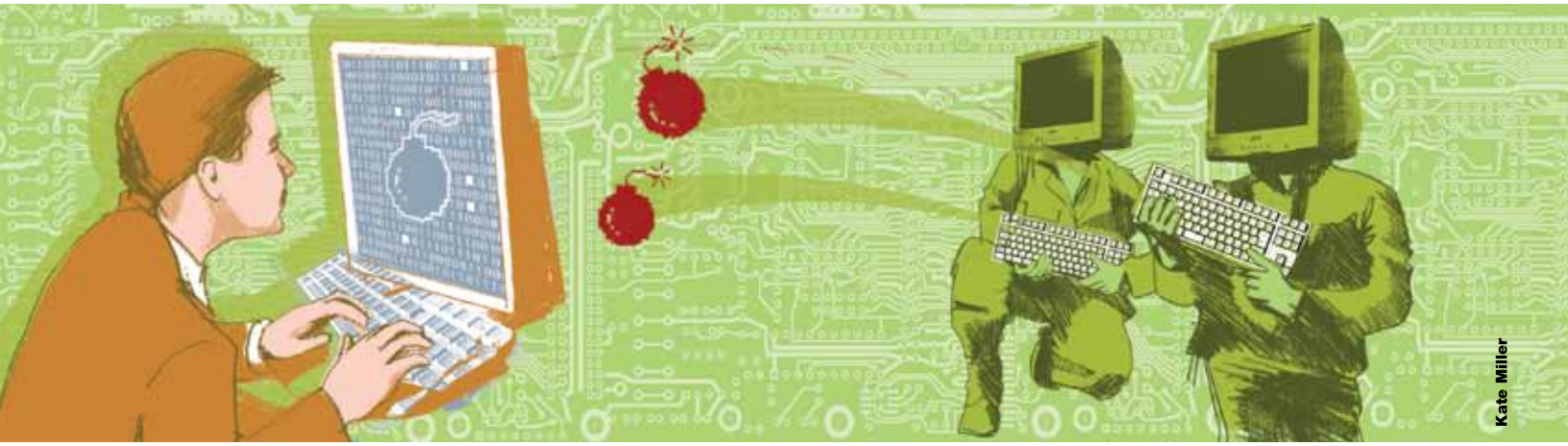


BUSINESS TECHNOLOGY OFFICE

Playing war games to prepare for a cyberattack

A poor response can be far more damaging than the attack itself.

Tucker Bailey, James Kaplan, and Allen Weinberg

"Can it happen to us?" All over the world, technology executives have been fielding this question from boards of directors and CEOs in the wake of highly publicized cyberattacks on large, well-respected companies and public institutions.

"Yes" is the only honest answer at a time when ever more value is migrating online, when business strategies require more open and interconnected technology environments, when attackers have always-expanding capabilities, and when attacks take advantage of limited security awareness among employees and customers. In fact, it may already have happened to you—but you may not know it.

Although political "hacktivists," such as Anonymous and LulzSec, certainly delight in announcing their exploits to the world and causing embarrassment to their targets, other sophisticated attackers seek to cover their tracks. Organized-crime rings engaging in cyberfraud have no interest in letting their targets know they have been infiltrated.

We believe that boards and senior business leaders should be asking the technology team a different question—namely, "Are we ready to respond to a cyberattack?"

An ill-thought-out response can be far more damaging than the attack itself. Whether customers cancel their accounts in the wake of a successful cyberattack depends as much on the quality of a company's communications as on the gravity of the breach. How much value is destroyed by the loss of sensitive business plans depends on the ability to adjust tactics quickly.

Takeaways

Many top executives are asking whether a cyberattack could hit their company—but they should instead be focusing on whether they are ready to respond to an attack.

Cyberwar games can test a company's readiness, for example, determining whether the security team could identify and assess a breach quickly; they also yield insights into security vulnerabilities and information assets that require protection.

Planning and conducting a cyberwar game can take 6 to 12 weeks, but doing so may build the company's ability to make decisions in real time with limited information.

Testing readiness with cyberwar games

The armed forces have long conducted war games to test capabilities, surface gaps in plans, and build their leaders' abilities to make decisions in real time. Some companies—3 percent, according to a recent McKinsey survey of digital business practices—have conducted cyberwar games to help ensure they are ready to manage a cyberattack. In fact, many corporate cyberwar-gaming efforts have been directly inspired by national-defense-oriented cyberwar games.

A cyberwar game is very different from traditional penetration testing, in which companies employ or contract with "white hat" hackers to identify technical vulnerabilities, such as unsecured network ports or externally facing programs that share too much information in the browser bar.

A cyberwar game is organized around a business scenario (such as cybercriminals using "spear phishing" attacks to target high-net-worth customers for fraud). It is structured to simulate the experience of a real attack. Participants receive incomplete information, and their objectives may not be 100 percent aligned. The simulation is cross-functional, involving participants from not only information security but also application development, technology infrastructure, customer care, operations, marketing, legal, government affairs, and corporate communications.

The cyberwar game occurs over a few days but requires up-front analysis of business-information assets and potential security vulnerabilities to make the scenario relevant and the game play realistic. The exercises usually do not affect live production systems; many cyberwar games are "tabletop" exercises.

Most important, a cyberwar game tests for flaws in a company's ability to react to an attack by answering key questions about the capabilities required for a successful response:

- Will the security team identify and assess the breach quickly?
  One organization found that the processes its security team used to address a breach were entirely dependent on e-mail and instant messaging; the organization would have limited ability to respond to an attack that compromised those systems.

- Will the team make effective decisions in containing the breach?
  One corporation discovered that it did not have functional guidelines for deciding when to shut down parts of its technology environment. It found that senior executives would have ordered the technology team to sever external connectivity unnecessarily, thereby preventing customers from accessing their accounts.

- Will the team effectively communicate the breach to the full set of stakeholders?
  At one financial institution, a war game demonstrated that guidelines had not been differentiated for communicating with customers whose data had been breached. As a result, high-net-worth customers would have received an impersonal e-mail.

- Can the company adjust business strategies and tactics in the wake of a breach?
  At one manufacturer, a war game revealed that business managers had never thought through what they would do if competitors or counterparties gained access to sensitive information, and so would be unable to change negotiation strategies quickly after the disclosure of proprietary information about their cost structure.

Exhibit 1

Cyberwar games yield insights into security vulnerabilities and information assets.

Assets		Sample threats
Individual data	**Customer data**	• In an "advanced persistent threat," **criminals** harvest customer data on an ongoing basis without being detected by IT security. • **Insider (developer)**[1] uses unsecured open-source plug-in, creating security breach. • **Hacktivists** initiate full data-center failure to showcase inefficiencies.
	Employee credentials	• **Criminals** with stolen employee credentials leverage poor physical security to get access to store location and harvest confidential data.
	Employee personal data	• **Hacktivists** steal senior-executive performance reviews from unstructured database server to showcase mismanagement.
Corporate information	**Confidential corporate information**	• **Criminals** steal confidential corporate information and sell it to financial-institution agents to be used in stock-arbitrage opportunity. • **Criminals** gain system access through iPad application and steal confidential information. • **Hacktivists** steal confidential data as they are transferred across divisions or borders.
	Stakeholder information	• **Criminals** steal stakeholder information from third-party-service cloud infrastructure and sell it to competition.
	Intellectual property	• **Insider (disgruntled employee)** gains access to key pricing data and sells to competitor, who can then systematically underprice for selected segments or regions.
	Marketing assets[2]	• **Insider (disgruntled employee)** sells information on breakthrough product to competitors.

[1] In this case, the attacker is an employee who has made a mistake or created a breach by accident.
[2] Including product information and sales strategy.

Gaining insights from gaming

Cyberwar games yield insights into information assets that require protection, security vulnerabilities that attackers can exploit, and flaws (or "failure modes") in a corporation's ability to respond to an attack (Exhibit 1).

The analysis required to develop relevant scenarios for the war game also facilitates a discussion between business and security managers about which risks and types of information assets are most important, who would want to compromise these information assets, and what the implications of an attack could be with regard to loss of intellectual property, loss of reputation, business disruption, or fraud. This information is not always clear before such a discussion. For example, one public institution found out that most of its IT-security processes were geared toward preventing online fraud, even though the biggest risk was the loss of confidence associated with a public breach.

Likewise, the analysis required to ensure that scenarios used in the game are realistic can, in turn, highlight important security risks. For instance, one retail brokerage discovered that most of its most sensitive information assets were hosted on applications that had not undergone security reviews and used out-of-date controls for authenticating users.

Conducting a cyberwar game

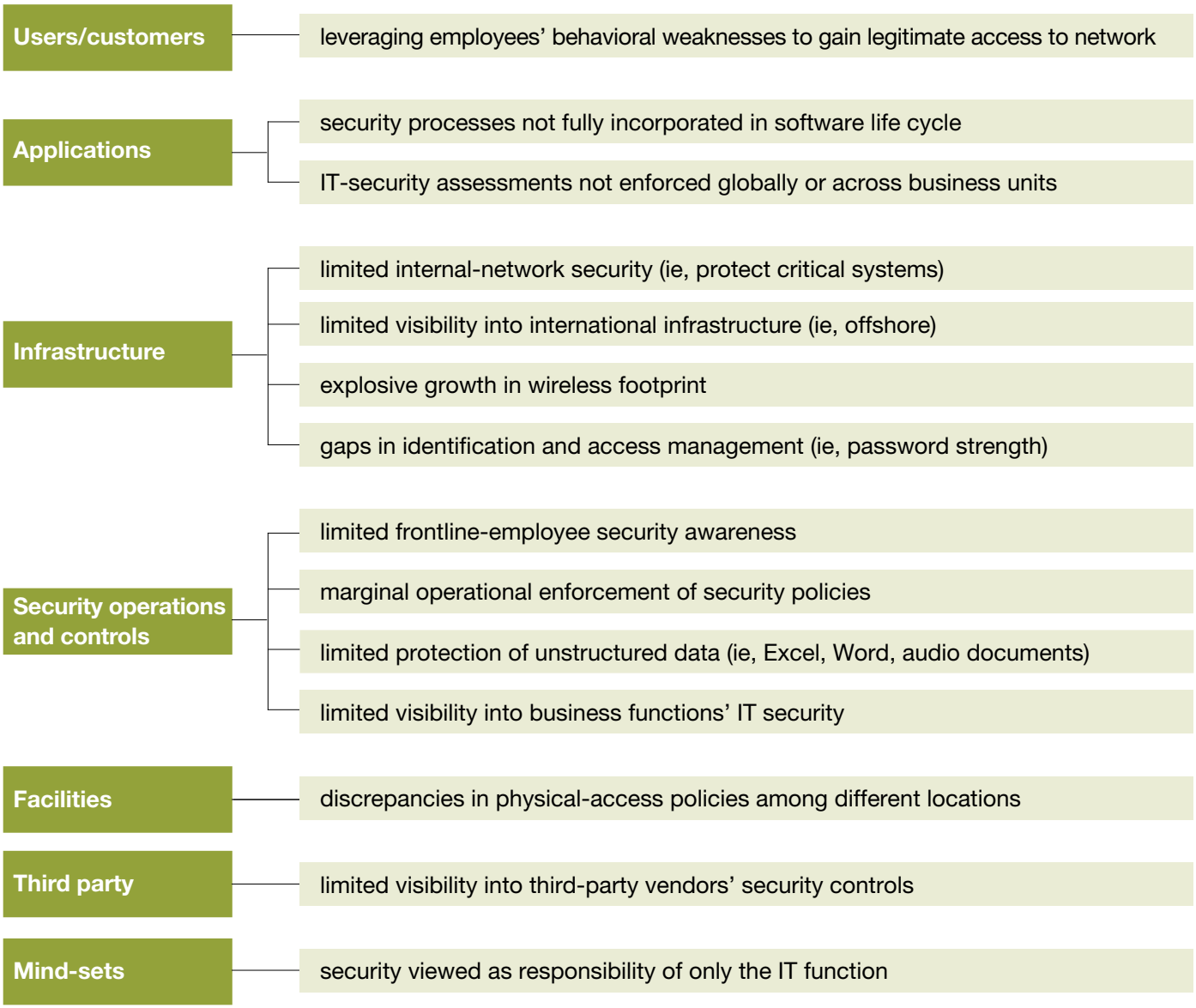
Most corporations can plan and conduct a game in 6 to 12 weeks, with a manageable impact on security, technology, and business managers' time.

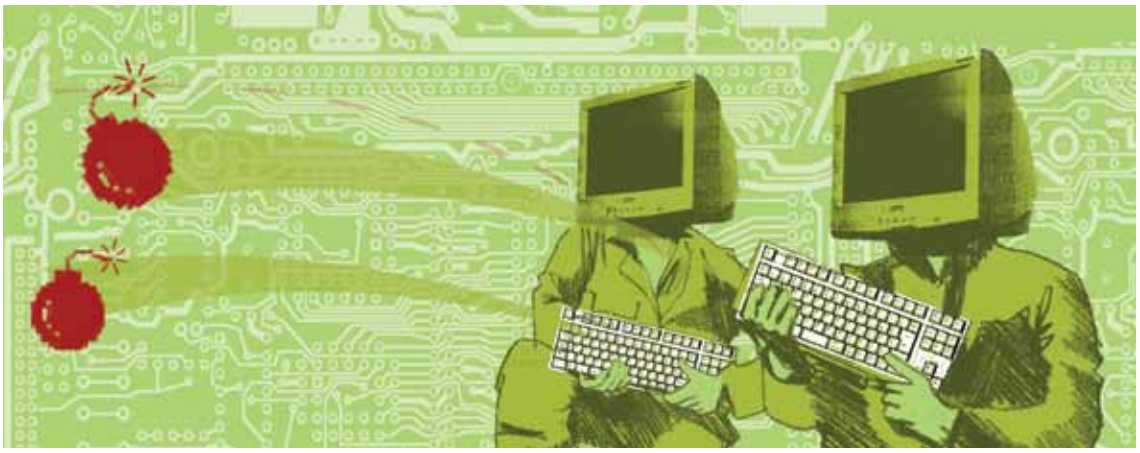
Aligning the scope and objectives of the war game is the first step. This includes deciding how many scenarios to incorporate into the game, how sophisticated those exercises will be, and how much participation will be required of the representatives of each business function who

Exhibit 2

Preparation for cyberwar games surfaces vulnerabilities that can then be tested.

Examples of IT-security vulnerabilities





help design the game. These "trusted agents" develop potential scenarios that take into account critical information assets, attackers who would want to compromise them, and any existing security vulnerabilities they might exploit (Exhibit 2).

After selecting the scenarios to be deployed in the game, the agents identify the failure modes they need to test for and create the step-by-step script that a facilitator—an internal or external war-gaming expert—uses when running the game.

The simulation or game itself can last anywhere from a day to a week or more, depending on the complexity of the scenarios. Throughout the course of the simulation, the facilitator will provide participants with intermittent updates or new information on which they can act. At each turn, the data that the players representing functions like security, marketing, and legal receive depend on the actions they have just taken.

The last and most important phase takes the insights generated by the simulation and converts them into actionable steps that will improve a corporation's ability to respond to an attack. These steps typically include everything from implementing tools that increase an organization's ability to foresee attacks, clarify responsibilities, and develop guidelines for making high-stakes decisions under pressure to creating communications protocols that can be pulled "off the shelf" when required.

• • •

Conducting a war game to test a corporation's ability to manage a cyberattack requires genuine effort and planning. However, it is one of the most effective mechanisms for prioritizing which assets to protect, surfacing vulnerabilities, identifying flaws in a company's ability to respond, and building the type of "muscle memory" required to make appropriate decisions in real time with limited information.

Tucker Bailey (Tucker_Bailey@McKinsey.com) is an associate principal in McKinsey's Washington, DC, office; **James Kaplan** (James_Kaplan@McKinsey.com) is a principal in the New York office, where **Allen Weinberg** (Allen_Weinberg@McKinsey.com) is a director.