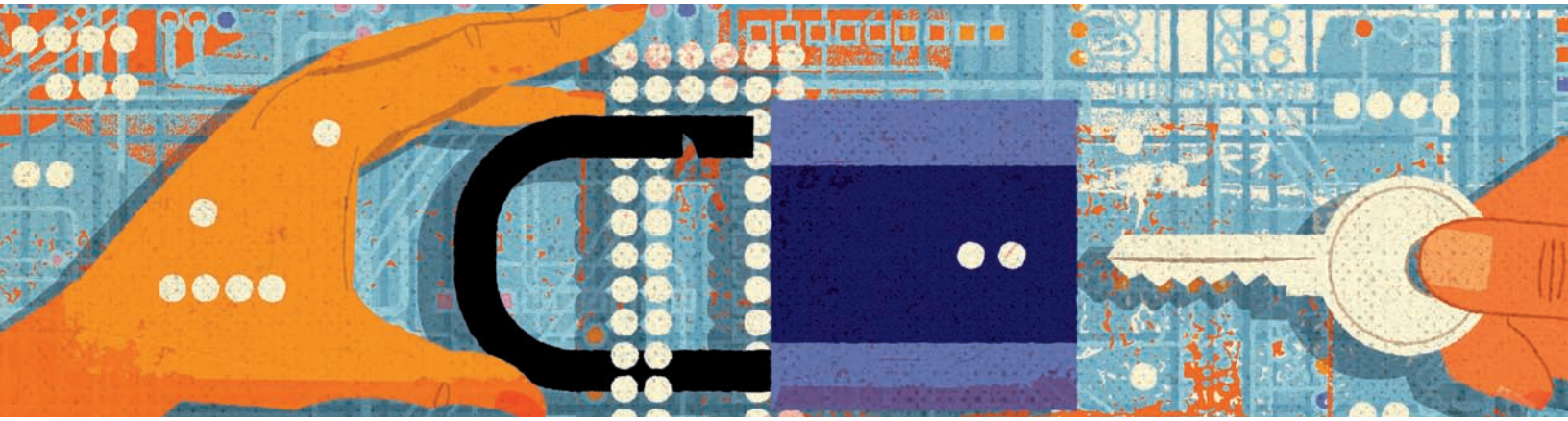


Can you hack it?
Managing the cybersecurity challenge

To secure cyberspace, technology alone is not enough. Strong management plays an equally important role.

John Dowdy, Joseph Hubback, Dennis Layton, and James Solyom

Cyberspace, according to the US government, is "the interdependent network of information technology infrastructures," including "the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries."[1] Governments and corporations worldwide are beginning to recognize the fact that securing cyberspace—protecting its confidentiality, integrity, and availability—is of paramount importance.

In its 2009 cyberspace policy review, the Obama administration asserted that "threats to cyberspace pose one of the most serious economic and national security challenges of the 21st century for the United States and our allies."[2]

Europe has similar concerns: the United Kingdom's National Security Strategy, for example, cites "hostile attacks upon UK cyberspace by other states and large-scale cyber crime" as a Tier 1 threat.[3]

Yet governments today have a poor understanding of the cybersecurity landscape and the scale of the challenge. One reason for this lack of clarity is that the term "cyberattack" is often used to describe everything from low-probability catastrophic events (such as devastating attacks on infrastructure) to higher-frequency threats (such as cyberespionage and intellectual-property theft). In addition, there is a dearth of reliable data on the economic cost of attacks on government. Most top-down estimates of the scale of the issue

[1] National Security Presidential Directive 54 and Homeland Security Presidential Directive 23, as per *Cyberspace policy review*, p. 1.
[2] Ibid.
[3] *A strong Britain in an age of uncertainty: The national security strategy*, UK government, October 2010.

are based primarily on questionable assumptions that yield implausible figures[4] and thus do not offer a sound basis for decisions about policy or government interventions.

In this article, we propose a cybersecurity taxonomy to help government leaders understand the landscape, and a "value at risk" framework that government leaders can use to prioritize and focus on the most serious threats. It is our firm belief that cybersecurity is first and foremost a management problem, not simply a technical problem, and therefore our taxonomy and framework take a senior-management perspective. We also outline four principles for a best-practice management response to cyberthreats. Adhering to these principles will enable government to act as an effective protector of valuable assets.

Understanding the landscape and the value at risk

We have developed a six-part taxonomy of the cybersecurity problem (Exhibit 1). The logic behind our taxonomy is that an attack will occur if an attacker has both the capability and the incentive to strike at vulnerabilities in a target's assets. Today, attackers' capabilities and incentives are increasing—the former due to technological developments and the latter due to the fact that more data and assets are now accessible online.[5] The relative lack of traceability means that attackers continue to feel little threat of retribution. Meanwhile, targets' vulnerabilities are decreasing, but at a slower pace than the increase in attackers' capabilities, which suggests that attacks will continue to increase in frequency and impact.

The taxonomy is helpful for understanding the cybersecurity landscape, but to identify and plan for the most serious threats, government leaders must be able to quantify the impact of attacks. What, for example, was the cost of the alleged loss of data relating to the F-35 Joint Strike Fighter? What was the cost to the US government of the release of its data by Wikileaks? There is a lack of data, from private enterprise or government, to help answer these questions. Various estimates put the direct cost of a cyberattack on a large company at between $1.6 million and $7.2 million.[6] At the extreme, the reported attacks on the F-35 program could compromise the US government's estimated $323 billion development cost.[7]

Extrapolating such estimates into economy-wide figures is problematic. How many attacks of this magnitude occur, and with what regularity? In a 2011 survey, more than 80 percent of critical-infrastructure providers reported being the victim of large-scale cyberattacks or infiltrations.[8] And many incidents that are detected go unreported, in part because reporting requirements vary by jurisdiction but also because there are clear disincentives—especially for corporations—to report breaches.

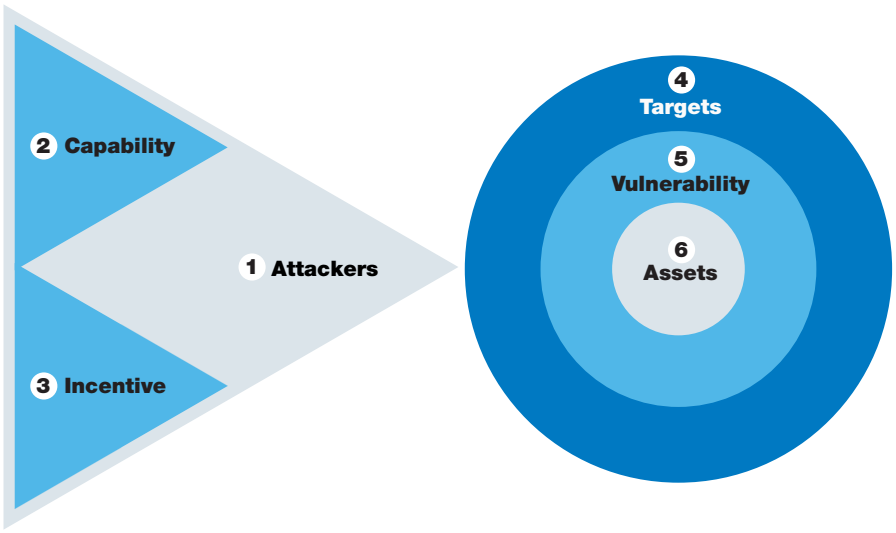
We have used our taxonomy to create a relative value-at-risk analysis that offers government leaders insights into the likelihood and impact of

[4] See "Sex, lies and cyber-crime surveys," Dinei Florêncio and Cormac Herley, Microsoft Research, June 2011.
[5] For more on the impact of ever-increasing amounts of data, see *Big data: The next frontier for innovation, competition, and productivity*, McKinsey Global Institute, May 2011.
[6] Ponemon Institute 2009 Annual Study: "Cost of a data breach"; *Symantec Internet Security Threat Report 2010*, PricewaterhouseCoopers Information Security Breaches survey, 2010.
[7] US General Accounting Office, "Testimony before the Subcommittees on Air and Land Forces and Seapower and Expeditionary Forces, Committee on Armed Services, U.S. House of Representatives," GAO-10-478T, March 24,2010.
[8] McAfee and Center for Strategic and International Studies (CSIS), "In the dark: Crucial industries confront cyberattacks," 2011.

To identify and plan for the most serious threats, government leaders must be able to quantify the impact of attacks

Exhibit 1

The taxonomy of cybersecurity helps government leaders understand the landscape.



1 Four groups of attackers[1]
a. Governments
b. Enterprises
c. Cybercriminals
d. Cyberterrorists or "hacktivists"

2 Capability
The ability to steal, hijack, impair, or damage

3 Incentive
The motive to attack

4 Four types of target entity
a. Public sector
b. Private enterprise
c. Individuals
d. Critical national infrastructure (CNI)

5 Vulnerability
Can be technical (eg, lack of a firewall) or human (eg, employees being tricked by phishing e-mails)

6 Assets
a. Data (such as IP[2], customer records, or classified national secrets)
b. Systems, which vary in criticality from low (eg, informational Web sites) to high (eg, nuclear monitoring systems)

[1]Members of multiple groups can work together in a single attack, in either a coordinated or an uncoordinated way.
[2]Intellectual property.

attacks for each combination of attacker and target (Exhibit 2). We see value at risk as a combination of three elements: the attacker's capability, the asset's vulnerability, and the relative financial and nonfinancial costs of the attack. Our estimates of relative costs—which take into account financial value but also factors such as national security and the protection of civil liberties—were informed by available data, our experience working in both the public and private sectors, and extensive interviews with leaders and IT specialists worldwide.

As the exhibit shows, the highest value at risk applies to enterprise-held intellectual property (IP). IP is both extremely valuable and

Exhibit 2

A value-at-risk analysis offers insights into where the most serious threats are.

Estimation of value at risk relative to existing protection
- Low
- Medium
- High

An attack could be consistent with the attacker's incentives
- ●

		Targets and assets								
Attackers	**Incentives**	**Public sector**			**Private enterprise**			**CNI**[2]	**Individuals**	
		Classified information	Sensitive information	Systems	IP[1]	Non-IP data	Systems	Systems	Personal information	Systems
Government	Strategic advantage	●	●	●	●	●	●	● War	●	●
Private enterprise	Financial gain	●	●		●	●		●	●	
Cyber-criminals	Financial gain	●	●	●	●	●	●	●	●	●
Cyber-terrorists, hacktivists	Protest, fun, terror	●	●	●	●	●	●	●		●

[1]Intellectual property.
[2]Critical national infrastructure (eg, power station).

vulnerable. It is easily stolen from electronic systems, often without the theft even being noticed. We estimate the value of the S&P 500's IP to be between $600 billion and $1.2 trillion.[9] Governments have a critical interest in ensuring the protection of IP due to its importance to both economic growth and the government's own defense investments (for example, IP held by defense suppliers).

Medium value-at-risk attacks should be a second-level priority. In the private sector, these are primarily attacks on non-IP assets, such as customer data. Another medium value-at-risk concern: the threat from foreign governments to critical national infrastructure (CNI). Here, the very high relative costs are dispersed across a wide range of assets, locations, and sectors, thus reducing the risk of a catastrophic attack. Furthermore, given that the primary threat to CNI is from other governments, an attack on CNI systems could be construed as an act of war—and is therefore less likely, as there are implicit retaliatory threats already in place.

Another group of medium value-at-risk assets consists of government systems and classified data. For example, we estimate the UK public

[9]Based on discounted value of research-and-development expenditures and corroborated by the value of intellectual-property-relevant intangible assets on S&P 500 balance sheets.

sector's maximum loss from cyber-enabled fraud to be $5.2 billion.[10] Although significant, this figure is small in comparison with the value at stake for private-sector IP losses. Furthermore, most governments already invest heavily in reducing the vulnerability of internal data, thus reducing the risk of attack.

A management challenge

Responding to the threat of cyberattacks requires more than simply increasing spending on technical defense mechanisms such as firewalls and antivirus software. It requires senior-management attention and a broad range of both technical and nontechnical capabilities.

There are four principles that underlie a best-practice management response to the cybersecurity threat. They apply equally at any level of government; the assurance questions for each principle enable all managers to test the effectiveness of their response.

Define and prioritize risks

"*Do we have a clear understanding of our portfolio of network-enabled assets and their respective value at risk? Do we have sufficiently robust best practices and expertise in-house to adequately protect them?*"

To manage a cybersecurity program effectively, leaders must clearly define what they are protecting and prioritize the threats they face. We suggest a three-step process to define and prioritize risks.

The first step is to conduct an organization-wide asset audit. Leaders must identify the assets—normally, the data and systems—that could be at risk from a cyberattack. The audit should encompass the entire spectrum of network-enabled assets, including those that may not traditionally be seen as at risk (such as systems that are not online but that may be connected to the outside world through USB ports). The audit should also consider assets held by other organizations, especially suppliers. The alleged compromise of the F-35 plans, for example, followed intrusions into the systems of two or three contractors rather than the systems belonging to the Department of Defense (DOD).[11]

The second step is to conduct a risk assessment to gauge the impact and likelihood of attacks on each asset. The organization should estimate both financial and reputational impact using a relative scale (such as a simple low/medium/high). A distributed denial-of-service (DDOS) attack on the Treasury Department's Web site, for instance, may rank low for financial impact and medium for reputational impact. Then, for each asset, the organization should estimate the likelihood of a successful attack, again using a relative scale—taking into account the attacker's incentive, the attacker's capability, and the target's vulnerability. For example, a DDOS attack on the Treasury Web site may be rated high for attacker incentive and capability and medium for vulnerability.

The third step is to categorize assets according to value at risk. Often two categories will suffice: lower value-at-risk assets (such as informational Web sites), which existing best practice should cover, and higher value-at-risk assets (such as vital systems), which require additional measures. Some of these measures—more advanced security and vulnerability management, for example—may involve building deep internal expertise or contracting for external assistance.

[10] McKinsey analysis based on *National Fraud Authority Report*, 2010, Her Majesty's Revenue and Customs data.
[11] "Computer spies breach fighter-jet project," *The Wall Street Journal*, April 21, 2009.

Assign responsibility for cyberthreat mitigation

"Who are the named and empowered individuals responsible for our highest-priority network-enabled assets? Who is responsible for setting and executing our cybersecurity strategy? What is the process for linking those individuals so that we have a consistent and coordinated approach that does not undermine the efficiency of our operations?"

Cybersecurity is a cross-functional issue. Organization-wide responsibility for policy should rest with a board member of the department or agency. Below board level, organizations should clearly define responsibility for cybersecurity so that they can take a comprehensive series of actions to mitigate threats.

Leaders should assign responsibility for cybersecurity in three areas. Ownership of each area may be delegated to the relevant department (for instance, the human-resources director could be accountable for people policies). The three areas are as follows:

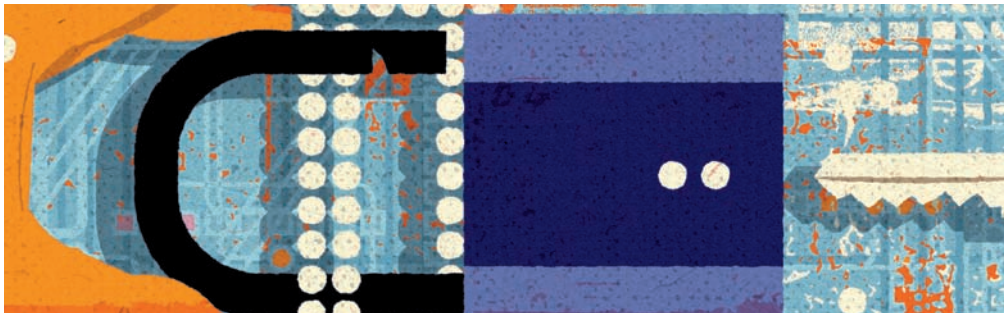
Technology. Technology must be used to maximum advantage to counter cyberattacks. The organization must have the level of technical capabilities required and should prioritize technical spending in the areas of highest risk. Basic security best practices should be embedded within the architecture (for example, limiting administrator rights or conducting simulations of cyberattacks to test resilience).

Process and procedure. Procedures must be established to limit and mitigate the impact of attacks. Responsibility in this area includes ensuring that information about attacks is available to leaders within the business (for example, predictive threat analysis based on aggregating and analyzing e-mail headers) and that data assets are suitably categorized (for example, working with business owners to determine appropriate encryption levels).

People. Personnel policies must be in place to minimize risk. This includes providing training to support the policy and regularly testing compliance.

Supplementing the organization-wide policies, leaders should assign high-risk assets to individuals to ensure that cybersecurity threats are seen as a business risk rather than simply an IT problem—for example, protection of health records may be the responsibility of an operations manager. The risk owner, however, should not be the same person who has business responsibility for an asset, so as to avoid conflicting incentives or priorities: an owner of classified data, for example, may want to improve functionality by combining data sets—at the expense of security.[12]

[12] For some threats, additionally assigning responsibility by threat vector may be appropriate—giving (often technical) teams or individuals the responsibility of tackling a particular threat (for example, distributed denial-of-service attacks across all Web sites operated by a government department).



Manage the performance of those responsible

"What is the basis for managing the performance of those responsible for the protection of our network-enabled assets? How are we performing against those assessments?"

Key performance indicators (KPIs) for the individuals responsible for cybersecurity should include metrics mirroring the three areas for threat mitigation, as follows:

Technological KPIs. These KPIs point to the number and type of electronic touchpoints, both internal and external, and highlight the quality of management of these connections. An example of such a KPI is the number of days that elapse between Microsoft issuing a critical software update and the entire organization installing it.

Process and procedural KPIs. These KPIs can include data-policy indicators that measure the success of data segmentation and risk-assessment activities (for example, the proportion of data that are suitably encrypted) and operational-policy indicators that measure the implementation success of policy (for example, the number of attempted security-policy breaches within a certain period).

People KPIs. People KPIs measure the success rate of training, employee conformity to security guidelines, or employee knowledge and use of best-practice e-mail behavior. They may be assessed through spot tests.

To support these KPIs, organizations should put in place a performance-management review system and a set of incentives and consequences. Organizations should also ensure accurate flow of information on the frequency and type of attacks, as well as on compliance with management practices.

Develop a cyberattack contingency plan

"What is our plan if we experience a significant security breach? How will we communicate internally and externally?"

Governments must have a robust response plan in the event of a successful cyberattack. A best-practice plan includes three phases: crisis management, recovery, and postmortem.

The first phase is immediate crisis management, or how the organization should respond when it detects an attack. This should feature two elements: a communications response and a system response, both of which should be proportionate to the impact of the attack.

The communications response, typically owned by the head of public relations, should aim to give stakeholders the information they need to know. This is particularly important for governments, given the likelihood of media and public interest. Key stakeholders will vary depending on the area of government attacked and should be identified in advance. For example, if there is an attack on a system for sharing patient information among hospitals, the stakeholders may include hospital staff, nonhospital doctors, patients, data-protection authorities, and other organizations using similar systems. Immediately following a DDOS attack on its Web site, the United Kingdom's Serious Organised Crime Agency (SOCA) promptly issued a media statement describing the extent of the attack and informing the public that it had taken its Web site offline.[13] Some news reports characterized the attack itself as embarrassing for SOCA, but its communications response was best practice.

The system response, the main goal of which is to terminate or ring-fence the breach, is normally owned by the head of IT. Again, the response

[13] "Soca website taken down after LulzSec 'DDoS attack,'" BBC News, June 20, 2011.

should be commensurate with the impact of the attack. For example, an agency should not necessarily sever its IT communication links for a relatively low-level DDOS attack—but it may want to cut off access in the event of a significant intrusion or hijack of its systems. Organizations should codify and practice these measures beforehand, not develop them on the fly. Once an organization contains the breach, it should initiate backup systems (such as a mirror Web site). A crucial part of the system response should be to inform IT departments in other government organizations of the nature of the attack so that they can upgrade their protection. For example, detection of a targeted phishing attack on the DOD should trigger a warning to all other US government departments.

The second phase is recovery, which is predominantly a technical response that builds on the immediate system response in the previous phase. The purpose is to repair damaged systems and data, fix the vulnerability that led to the attack, and bring systems back online. An ineffective recovery response leaves the target exposed to more attacks, which can lead to further embarrassment and cost.

The third phase is the postmortem, normally enacted by the corporate risk owner. The purpose of the postmortem is self-evaluation: to flush out the causes of the attack and prevent a similar one from recurring, to investigate attackers and their motives and explore opportunities for restitution, and to evaluate the success of the response plan. The response plan should include a board-level report that details the agreed-on actions to be taken, with clear time frames and owners for each. A successful postmortem may include supporting a criminal investigation.

• • •

Cybersecurity is a growing and ever-changing challenge. Government responses and policies regarding cybersecurity should not be static but instead should be continually adapted and refreshed as new knowledge becomes available. While existing efforts to share knowledge among organizations (such as the forums hosted by the US Office of Cybersecurity and Communications) are laudable, there is still too little knowledge sharing when it comes to cybersecurity, resulting in organizations not being as well prepared for attacks as they could be. A greater level of collaboration is particularly important among leading targets such as governments, advanced industries, and financial institutions. Within the public sector, sharing should happen at many levels—not only shared information and shared storytelling but shared action as well—reflecting the interconnectedness of government departments.

John Dowdy is the global leader of McKinsey's Aerospace and Defense practice. He is a director in the London office, where **Joseph Hubback** and **James Solyom** are consultants and **Dennis Layton** is a principal. The authors wish to thank Tucker Bailey, Assaf Egozi, Scott Gebicke, James Kaplan, Edward Lock, Chris Rezek, Giacomo Sonnino, and Allen Weinberg for their contributions to this article.