by James A. "Sandy" Winnefeld Jr., Christopher Kirchhoff, and David M. Upton

CYBERSECURITY'S HUMAN FACTOR: LESSONS FROM THE PENTAGON

The vast majority of companies are more exposed to cyber-attacks than they have to be. To close the gaps in their security, CEOs can take a cue from the U.S. military. Once a vulnerable IT colossus, it is becoming an adroit operator of well-defended networks. Today the military can detect and remedy

MICHAEL BYERS

intrusions within hours, if not minutes. From September 2014 to June 2015 alone, it repelled more than 30 million known malicious attacks at the boundaries of its networks. Of the small number that did get through, fewer than 0.1% compromised systems in any way. Given the sophistication of the military's cyberadversaries, that record is a significant feat.

One key lesson of the military's experience is that while technical upgrades are important, minimizing human error is even more crucial. Mistakes by network administrators and users—failures to patch vulnerabilities in legacy systems, misconfigured settings, violations of standard procedures—open the door to the overwhelming majority of successful attacks.

The military's approach to addressing this dimension of security owes much to Admiral Hyman Rickover, the "Father of the Nuclear Navy." In its more than 60 years of existence, the nuclear-propulsion program that he helped launch hasn't suffered a single accident. Rickover focused intensely on the human factor, seeing to it that propulsion-plant operators aboard nuclear-powered vessels were rigorously trained to avoid mistakes and to detect and correct anomalies before they cascaded into serious malfunctions. The U.S. Department of Defense has been steadily adopting protocols similar to Rickover's in its fight to thwart attacks on its IT systems. Two of this article's authors, Sandy Winnefeld and Christopher Kirchhoff, were deeply involved in those efforts. The article's purpose is to share the department's approach so that business leaders can apply it in their own organizations.

Like the Defense Department, companies are under constant bombardment from all types of sources: nation-states, criminal syndicates, cybervandals, intruders hired by unscrupulous competitors, disgruntled insiders. Thieves have stolen or compromised the credit-card or personal information of hundreds of millions of customers, including those of Sony, Target, Home Depot, Neiman Marcus, JPMorgan Chase, and Anthem. They've managed to steal proprietary information on oil and gas deposits from energy companies at the very moment geological surveys were completed. They've swiped negotiation strategies off internal corporate networks in the run-up to major deals, and weapons systems data from defense contractors. And over the past three years intrusions into critical U.S. infrastructure—systems that control operations in the chemical, electrical, water, and transport sectors—have increased 17-fold. It's little wonder, then, that the U.S. government has made improving cybersecurity in both public and private sectors a national priority. But, as the recent hacking of the federal government's Office of Personnel Management underscores, it is also a monumental challenge.

The Military's Cyberjourney

Back in 2009, the Defense Department, like many companies today, was saddled with a vast array of disparate IT systems and security approaches. Each of its three military branches, four uniformed services, and nine unified combatant commands had long functioned as its own profit-and-loss center, with substantial discretion over its IT investments. Altogether, the department comprised 7 million devices operating across 15,000 network enclaves, all run by different system administrators, who configured their parts of the network to different standards. It was not a recipe for security or efficiency.

That year, recognizing both the opportunities of greater coherency and the need to stem the rise in harmful incidents, Robert Gates, then the secretary of defense, created the U.S. Cyber Command. It brought network operations across the entire .mil domain under the authority of one four-star officer. The department simultaneously began to

Idea in Brief

THE PROBLEM

Cyberattacks are soaring. And—as companies like Sony, Target, Home Depot, Anthem, and JPMorgan Chase know all too well—they're succeeding. Most often, the cause is not inadequate security technology but mistakes by network administrators and users.

THE SOLUTION

Become a high-reliability organization—something the U.S. military is doing. It has made great strides in stopping attacks on its systems and quickly containing the few intrusions that occur. The key is creating a zero-defect culture like the one that Admiral Hyman Rickover implanted in the U.S. nuclear navy.

THE PRINCIPLES

To weed out and contain human error, organizations must embrace six principles: integrity, depth of knowledge, procedural compliance, forceful backup, a questioning attitude, and formality in communication.

consolidate its sprawling networks, collapsing the 15,000 systems into a single unified architecture called the Joint Information Environment. The work has been painstaking, but soon ships, submarines, satellites, spacecraft, planes, vehicles, weapons systems, and every unit in the military will be linked in a common command-and-control structure encompassing every communication device. What once was a jumble of more than 100,000 network administrators with different chains of command, standards, and protocols is evolving toward a tightly run cadre of elite network defenders.

At the same time, the U.S. Cyber Command has been upgrading the military's technology. Sophisticated sensors, analytics, and consolidated "security stacks"—suites of equipment that perform a variety of functions, including big data analytics—are giving network administrators greater visibility than ever before. They can now quickly detect anomalies, determine if they pose a threat, and alter the network's configuration in response.

The interconnection of formerly separate networks does introduce new risks (say, that malware might spread across systems, or that a vulnerability in one system would allow someone to steal data from another). But these are greatly outweighed by the advantages: central monitoring, standardized defenses, easy updating, and instant reconfiguration in the event of an attack. (Classified networks are disconnected from unclassified networks, of course.)

However, unified architecture and state-of-the-art technology are only part of the answer. In nearly all penetrations on the .mil network, people have been the weak link. The Islamic State briefly took control of the U.S. Central Command's Twitter feed in 2015 by exploiting an individual account that had not been updated to dual-factor authentication, a basic measure requiring users to verify their identity by password plus a token number generator or encrypted chip. In 2013 a foreign nation went on a four-month spree inside the U.S. Navy's unclassified network by exploiting a security flaw in a public-facing website that the navy's IT experts knew about—but failed to fix. The most serious breach of a classified network occurred in 2008, when, in a violation of protocol, a member of the Central Command at a Middle Eastern base inserted a thumb drive loaded with malware directly into a secure desktop machine.

While the recent intrusions show that security today is by no means perfect, the human and technical performance of the military's network administrators and users is far stronger by a number of measures than it was in 2009. One benchmark is the results of commands' cybersecurity inspections, whose numbers have increased from 91 in 2011 to an expected 285 in 2015. Even though the grading criteria have become more stringent, the percentage of commands that received a passing grade—proving themselves "cyber-ready"—has risen from 79% in 2011 to over 96% this year.

THE U.S. DEPARTMENT OF DEFENSE EXPERIENCES 41M SCANS, PROBES, AND ATTACKS A MONTH.

Companies need to address the risk of human error too. Hackers penetrated JPMorgan Chase by exploiting a server whose security settings hadn't been updated to dual-factor authentication. The exfiltration of 80 million personal records from the health insurer Anthem, in December 2014, was almost certainly the result of a "spear phishing" e-mail that compromised the credentials of a number of system administrators. These incidents underscore the fact that errors occur among *both* IT professionals and the broader workforce. Multiple studies show that the lion's share of attacks can be prevented simply by patching known vulnerabilities and ensuring that security configurations are correctly set.

The clear lesson here is that people matter as much as, if not more than, technology. (Technology, in fact, can create a false sense of security.) Cyberdefenders need to create "high-reliability organizations"—by building an exceptional culture of high performance that consistently minimizes risk. "We have to get beyond focusing on just the tech piece here," Admiral Mike Rogers, who oversees the U.S. Cyber Command, has said. "It's about ethos. It's about culture. [It's about] how you man, train, and equip your organization, how you structure it, the operational concepts that you apply."

The High-Reliability Organization

The concept of a high-reliability organization, or HRO, first emerged in enterprises where the consequences of a single error can be catastrophic. Take airlines, the air-traffic-control system, space flight, nuclear power plants, wildfire fighting, and high-speed rail. Within these highly technical operations, the interaction of systems, subsystems, human operators, and the external environment frequently gives rise to deviations that must be corrected before they become disastrous problems. These organizations are a far cry from continuously improving "lean" factories. Their operators and users don't have the luxury of learning from their mistakes.

Safely operating technology that is inherently risky in a dangerous, complex environment takes more than investing in the best engineering and materials. High-reliability organizations possess a deep awareness of their own vulnerabilities, are profoundly committed to proven operational principles and high standards, clearly articulate accountability, and vigilantly probe for sources of failure.

The U.S. Navy's nuclear-propulsion program is arguably the HRO with the longest track record. Running a nuclear reactor on a submarine deep in the ocean, out of communication with any technical assistance for long periods of time, is no small feat. Admiral Rickover drove a strict culture of excellence into each level of the organization. (So devoted was he to ensuring that only people who could handle such a culture entered the program that, during his 30 years at its helm, he personally interviewed every officer applying to join it—a practice that every one of his successors has continued.)

At the heart of that culture are six interconnected principles, which help the navy weed out and contain the impact of human error.

1. Integrity. By this we mean a deeply internalized ideal that leads people, without exception, to eliminate "sins of commission" (deliberate departures from protocol) and own up immediately to mistakes. The nuclear navy inculcates it in people from day one, making it clear there are no second chances for lapses. Workers thus are not only unlikely to take shortcuts but also highly likely to notify supervisors of any errors right away, so they can be corrected quickly and don't necessitate lengthy investigations later—after a problem has occurred. Operators of propulsion plants faithfully report every anomaly that rises above a low threshold of seriousness to the program's central technical headquarters. Commanding officers of vessels are held fully accountable for the health of their programs, including honesty in reporting.

2. Depth of knowledge. If people thoroughly understand all aspects of a system—including the

THE ANNUAL GLOBAL COST OF CYBERCRIME AGAINST CONSUMERS IS $113B.

SOURCE *2013 NORTON REPORT,* SYMANTEC
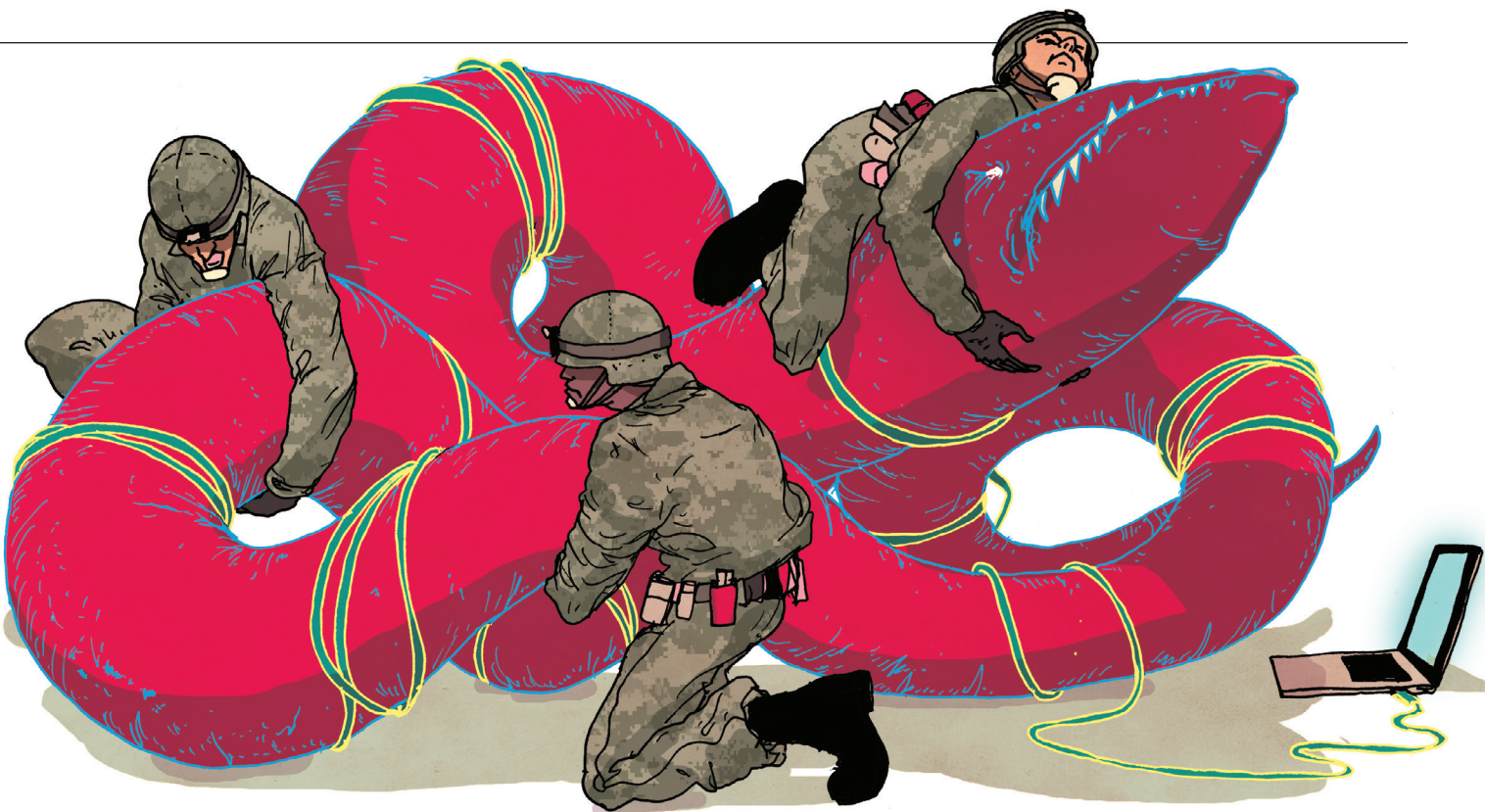
way it's engineered, its vulnerabilities, and the procedures required to operate it—they'll more readily recognize when something is wrong and handle any anomaly more effectively. In the nuclear navy, operators are rigorously trained before they ever put their hands on a real propulsion plant and are closely supervised until they're proficient. Thereafter, they undergo periodic monitoring, hundreds of hours of additional training, and drills and testing. Ship captains are expected to regularly monitor the training and report on crew proficiency quarterly.

3. Procedural compliance. On nuclear vessels, workers are required to know—or know where to find—proper operational procedures and to follow them to the letter. They're also expected to recognize when a situation has eclipsed existing written procedures and new ones are called for.

One of the ways the nuclear navy maximizes compliance is through its extensive system of inspections. For instance, every warship periodically undergoes tough Operational Reactor Safeguard Examinations, which involve written tests, interviews, and observations of day-to-day operations and of responses to simulated emergencies. In addition, an inspector from the Naval Reactors regional office may walk aboard anytime a ship is

in port, without advance notice, to observe ongoing power-plant operations and maintenance. The ship's commanding officer is responsible for any discrepancies the inspector may find.

4. Forceful backup. When a nuclear-propulsion plant is operating, the sailors who actually control it—even those who are highly experienced—are always closely monitored by senior personnel. Any action that presents a high risk to the system has to be performed by two people, not just one. And every member of the crew—even the most junior person—is empowered to stop a process when a problem arises.

5. A questioning attitude. This is not easy to cultivate in any organization, especially one with a formal rank structure in which immediate compliance with orders is the norm. However, such a mindset is invaluable: If people are trained to listen to their internal alarm bells, search for the causes, and then take corrective action, the chances that they'll forestall problems rise dramatically. Operators with questioning attitudes double- and triple-check work, remain alert for anomalies, and are never satisfied with a less-than-thorough answer. Simply asking why the hourly readings on one obscure instrument out of a hundred are changing in an abnormal way or

why a network is exhibiting a certain behavior can prevent costly damage to the entire system.

6. Formality in communication. To minimize the possibility that instructions are given or received incorrectly at critical moments, operators on nuclear vessels communicate in a prescribed manner. Those giving orders or instructions must state them clearly, and the recipients must repeat them back verbatim. Formality also means establishing an atmosphere of appropriate gravity by eliminating the small talk and personal familiarity that can lead to inattention, faulty assumptions, skipped steps, or other errors.

Cybersecurity breaches caused by human mistakes nearly always involve the violation of one or more of these six principles. Here's a sample of some the Defense Department uncovered during routine testing exercises:

- A polite headquarters staff officer held the door for another officer, who was really an intruder carrying a fake identification card. Once inside, the intruder could have installed malware on the organization's network. Principles violated: procedural compliance and a questioning attitude.
- A system administrator, surfing the web from his elevated account, which had fewer automatic restrictions, downloaded a popular video clip that was "viral" in more ways than one. Principles violated: integrity and procedural compliance.
- A staff officer clicked on a link in an e-mail promising discounts for online purchases, which was actually an attempt by the testers to plant a phishing back door on her workstation. Principles violated: a questioning attitude, depth of knowledge, and procedural compliance.

- A new network administrator installed an update without reading the implementation guide and with no supervision. As a result, previous security upgrades were "unpatched." Principles violated: depth of knowledge, procedural compliance, and forceful backup.
- A network help desk reset a connection in an office without investigating why the connection had been deactivated in the first place—even though the reason might have been an automated shutdown to prevent the connection of an unauthorized computer or user. Principles violated: procedural compliance and a questioning attitude.

Creating a High-Reliability IT Organization

To be sure, every organization is different. So leaders need to account for two factors in designing the approach and timetable for turning their companies into cybersecure HROs. One is the type of business and its degree of vulnerability to attacks. (Financial services, manufacturing, utility, and large retail businesses are especially at risk.) Another is the nature of the workforce. A creative workforce made up predominantly of Millennials accustomed to working from home with online-collaboration tools presents a different challenge from sales or manufacturing employees accustomed to structured settings with lots of rules.

It's easier to create a rule-bound culture for network administrators and cybersecurity personnel than it is for an entire workforce. Yet the latter is certainly possible, even if a company has a huge number of employees and an established culture. Witness the many companies that have successfully changed their cultures and operating approaches to increase quality, safety, and equal opportunity.

Whatever the dynamics of their organizations, leaders can implement a number of measures to embed the six principles in employees' everyday routines.

Take charge. A recent survey by Oxford University and the UK's Centre for the Protection of the National Infrastructure found that concern for cybersecurity was significantly lower among managers inside the C-suite than among managers outside it. Such shortsightedness at the top is a serious problem, given the financial consequences of cyberattacks. In a 2014 study by the Ponemon Institute, the average annualized cost of cybercrime incurred by a benchmark sample of U.S. companies was $12.7 million, a 96%

OVER THE PAST 3 YEARS, INTRUSIONS INTO CRITICAL U.S. INFRASTRUCTURE HAVE INCREASED 17X.

SOURCE U.S. DEPARTMENT OF DEFENSE

increase in five years. Meanwhile, the time it took to resolve a cyberattack had increased by 33%, on average, and the average cost incurred to resolve a single attack totaled more than $1.6 million.

The reality is that if CEOs don't take cybersecurity threats seriously, their organizations won't either. You can bet that Gregg Steinhafel, who was ousted from Target in 2014 after cybercriminals stole its customers' information, wishes he had.

Chief executives know that consolidating their jumble of network systems, as the Defense Department has done, is important. But many are not moving fast enough—undoubtedly because this task can be massive and expensive. In addition to accelerating that effort, they must marshal their entire leadership team—technical and line management, and human resources—to make people, principles, and IT systems work together. Repeatedly emphasizing the importance of security issues is key. And CEOs should resist blanket assurances from CIOs who claim they're already embracing high-reliability practices and say all that's needed is an increase in the security budget or the newest security tools.

CEOs should ask themselves and their leadership teams tough questions about whether they're doing everything possible to build and sustain an HRO culture. Are network administrators making sure that security functions in systems are turned on and up-to-date? How are spot audits on behavior conducted, and what happens if a significant lapse is found? What standardized training programs for the behavioral and technical aspects of cybersecurity are in place, and how frequently are those programs refreshed? Are the most important cybersecurity tasks, including the manipulation of settings that might expose the system, conducted formally, with the right kind of backup? In essence, CEOs must constantly ask what integrity, depth of knowledge, procedural compliance, forceful backup, a questioning attitude, and formality mean in their organizations. Meanwhile, boards of directors, in their oversight role, should ask whether management is adequately taking into account the human dimension of cyberdefense. (And indeed many are beginning to do this.)

Make everyone accountable. Military commanders are now held responsible for good stewardship of information technology—and so is everyone all the way down the ranks. The Defense Department and the U.S. Cyber Command are establishing a reporting system that allows units to track their security violations and anomalies on a simple scorecard. Before, information about who committed an error and its seriousness was known only to system administrators, if it was tracked at all. Soon senior commanders will be able to monitor units' performance in near real time, and that performance will be visible to people at much higher levels.

The goal is to make network security as much of an everyday priority for troops as keeping their rifles clean and operational. Every member of an armed service must know and comply with the basic rules of network hygiene, including those meant to prevent users from introducing potentially tainted hardware, downloading unauthorized software, accessing a website that could compromise networks, or falling prey to phishing e-mails. When a rule is broken, and especially if it's a matter of integrity, commanders are expected to discipline the offender. And if a climate of complacency is found in a unit, the commander will be judged accordingly.

Companies should do likewise. While the same measures aren't always available to them, all managers—from the CEO on down—should be responsible for ensuring their reports follow cybersafety practices. Managers should understand that they, along with the employees in question, will be held accountable. All members of the organization ought to recognize they are responsible for things they can control. This is not the norm in many companies.

Institute uniform standards and centrally managed training and certification. The U.S. Cyber Command has developed standards to ensure that anyone operating or using a military network is certified to do so, meets specific criteria, and is retrained at appropriate intervals. Personnel on dedicated teams in charge of defending networks undergo extensive formal training. For these cyberprofessionals the Defense Department is moving toward the model established by the nuclear navy: classroom instruction, self-study, and at the end of the process, a formal graded examination. To build a broad and deep pipeline of defenders, the military academies require all attendees to take cybersecurity courses. Two academies offer a major degree in cyberoperations, and two offer minor degrees. All services now have schools for advanced training and specific career paths for cybersecurity specialists. The military is also incorporating cybersecurity into continuing education programs for all personnel.

Relatively few companies, in contrast, have rigorous cybertraining for the rank and file, and those that do rarely augment it with refresher courses or information sessions as new threats arise. Merely e-mailing employees about new risks doesn't suffice. Nor does the common practice of requiring all employees to take an annual course that involves spending an hour or two reviewing digital policies, with a short quiz after each module.

Admittedly, more-intensive measures are time-consuming and a distraction from day-to-day business, but they're imperative for companies of all sizes. They should be as robust as programs to enforce ethics and safety practices, and companies should track attendance. After all, it takes only one untrained person to cause a breach.

Couple formality with forceful backup. In 2014 the U.S. military created a construct that spelled out in great detail its cyber-command-and-control structure, specifying who is in charge of what and at what levels security configurations are managed and changed in response to security events. That clear framework of reporting and responsibilities is supported with an extra safeguard: When security updates on core portions of the Defense Department's network are made or system administrators access areas where sensitive information is stored, a two-person rule is in effect. Both people must have their eyes on the task and agree that it was performed correctly. This adds an extra degree of reliability and dramatically reduces the risk of lone-wolf insider attacks.

There's no reason companies can't also do these things. Most large firms have already aggressively pruned their list of "privileged" system users and created processes for retracting the access rights of contractors leaving a project and employees leaving the firm. Midsize and smaller enterprises should do the same.

One form of backup can be provided by inexpensive, easy-to-install software that either warns employees when they're transferring or downloading sensitive information or prevents them from doing it and then monitors their actions. Regularly reminding employees that their adherence to security rules is monitored will reinforce a culture of high reliability.

Check up on your defenses. In June 2015 the U.S. Cyber Command and the Defense Department announced sweeping operational tests for both network administrators and users. The military also is establishing rigorous standards for cybersecurity inspections and tightly coordinating the teams that conduct them.

Companies should follow suit here as well. While many large firms do security audits, they often focus on networks' vulnerability to external attacks and pay too little attention to employees' behaviors. CEOs should consider investing more in capabilities for testing operational IT practices and expanding the role of the internal audit function to include cybersecurity technology, practices, and culture. (External consultants also may provide this service.)

In addition to scheduled audits, firms should do random spot-checks. These are highly effective at countering the shortcuts and compromises that creep into the workplace—like transferring confidential material to an unsecured laptop to work on it at home, using public cloud services to exchange sensitive information, and sharing passwords with other employees. Such behavior is important to discover—and correct—before it results in a serious problem.

Eliminate fear of honesty and increase the consequences of dishonesty. Leaders must treat unintentional, occasional errors as opportunities to correct the processes that allowed them to occur. However, they should give no second chances to people who intentionally violate standards and procedures. Edward Snowden was able to access classified information by convincing another civilian employee to enter his password into Snowden's workstation. It was a major breach of protocol for which the employee was rightfully fired. It made many military leaders realize that an operational

THE DEPARTMENT OF DEFENSE IS CONSOLIDATING 15,000 NETWORKS INTO A SINGLE UNIFIED ARCHITECTURE.

SOURCE U.S. DEPARTMENT OF DEFENSE

culture that stressed integrity, a questioning attitude, forceful backup, and procedural compliance could have created an environment in which Snowden would have been stopped cold. Such a breach of the rules would have been unthinkable in the reactor department of a navy vessel.

At the same time, employees should be encouraged to acknowledge their innocent mistakes. When nuclear-propulsion-plant operators discover a mistake, they're conditioned to quickly reveal it to their supervisors. Similarly, a network user who inadvertently clicks on a suspicious e-mail or website should be conditioned to report it without fear of censure.

Finally, it should be easy for everyone throughout the organization to ask questions. Propulsion-plant operators are trained to immediately consult a supervisor when they encounter an unfamiliar situation they aren't sure how to handle. Similarly, by ensuring that all employees can readily obtain help from a hotline or their managers, companies can reduce the temptation to guess or hope that a particular action will be safe.

Yes, we're calling for a much more formal, regimented approach than many companies now employ. With cyberthreats posing a clear and present danger to individual companies and, by extension, the nation, there is no alternative. Rules and principles are needed to plug the many holes in America's cyberdefenses.

Couldn't companies just focus on protecting their crown jewels? No. First, that would mean multiple standards for cybersecurity, which would be difficult to manage and, therefore, hazardous. Second, the crown jewels often are not what you think they are. (One could argue that the leak of embarrassing e-mails was the most damaging aspect of North Korean hackers' attack on Sony Pictures Entertainment.) Finally, hackers often can gain access to highly sensitive data or systems via a seemingly low-level system, like e-mail. A company needs a common approach to protecting all its data.

Technical Capability, Human Excellence

Over the past decade, network technology has evolved from a simple utility that could be taken for granted to an important yet vulnerable engine of operations, whose security is a top corporate priority. The soaring number of cyberattacks has made that abundantly clear. Technology alone can not defend a network. Reducing human errors is at least as important, if not more. Embracing the principles that an irascible admiral implanted in the nuclear navy more than 60 years ago is the way to do this.

Building and nurturing a culture of high reliability will require the personal attention of CEOs and their boards as well as substantial investments in training and oversight. Cybersecurity won't come cheap. But these investments must be made. The security and viability of companies—as well as the economies of the nations in which they do business—depend on it.

HBR Reprint R1509G

James A. "Sandy" Winnefeld Jr. was the ninth vice chairman of the U.S. Joint Chiefs of Staff and an admiral in the U.S. Navy until August, when he retired. **Christopher Kirchhoff** is a special assistant to the chairman of the Joint Chiefs of Staff. **David M. Upton** is the American Standard Companies Professor of Operations Management at Oxford University's Saïd Business School.