



Resilience in the Cyber Era

Building an Infrastructure that Secures and Protects

Economist Intelligence Unit

The Economist

An Economist Intelligence Unit research program sponsored by Booz Allen Hamilton

Booz | Allen | Hamilton



List of Interviewees

KAREN EVANS National Director,
U.S. Cyber Challenge

NIGEL INKSTER Director of Transnational
Threats and Political Risk, International
Institute for Strategic Studies

LINDA LAUN Global Business Continuity
and Resiliency Services Consulting Portfolio
and Methods Manager, IBM

LEN PADILLA Senior Director
of Technology, NTT Europe

ERNIE RAKACZKY Principal Security
Architect, Invensys

DAVE SCOTT Head of Solution
Consulting, NTT Europe

MICHAEL SHINN CEO, Prometheus Global

GARRY SIDAWAY Director of Security
Strategy, Integralis

JAMES P. G. STERBENZ Associate Professor,
Department of Electrical Engineering and
Computer Science, Communications and
Networking Systems Laboratory, University
of Kansas

About the Survey

In June and July 2011, the Economist Intelligence Unit conducted a global survey, sponsored by Booz Allen Hamilton, of 387 executives to assess attitudes toward cybersecurity, and their progress towards implementing resilience strategies. Nearly one-half (48 percent) of survey respondents are board members or C-level executives, including 92 CEOs. The respondents are based in Asia-Pacific (29 percent), North America (26 percent), Western Europe (26 percent), Latin America (9 percent), Middle East and Africa (7 percent) and Eastern Europe (3 percent). More than one-half of the survey respondents (55 percent) work for companies with global annual revenues exceeding US\$500 million. Nineteen different industries are represented in the survey sample, including financial services (20 percent), professional services (14 percent), energy and natural resources (12 percent), IT and technology (10 percent), and manufacturing (8 percent).

Contents

Executive Summary.....	2
Introduction	3
Resilience: Definitions Matter	5
The Proliferating Threat.....	6
The Corporate Response	7
The Government Response	9
Sidebar: The Role of Private Public Partnerships.....	10
Critical infrastructure issues: Developing Better System Architectures	10
Application issues: Resilience Through Better Software.....	11
Access issues: Greater Availability by Focusing on Data	12
Workforce issues: Becoming Resilience Aware.....	13
Sidebar: The Industry Differences	15
Conclusion	16
About Booz Allen	17
About Economist Intelligence Unit	17

Executive Summary

- **THE CYBER THREAT HAS EVOLVED FROM HACKERS FUNCTIONING AS HOBBYISTS TO SOMETHING MORE SERIOUS AND ORGANIZED.** Today's malicious agents are members of a growing industry of companies designed to infiltrate data centers to capture private information.
- **RESILIENCE CAN BE DEFINED** as the ability of a system or domain to withstand attacks or failures, and to reestablish itself quickly. But other definitions of resilience vary widely.
- **THE NEW ATTITUDE TOWARD RESILIENCE ACCEPTS THAT COMPANIES CANNOT ACHIEVE PERFECT SECURITY OR ABSOLUTE CONTINUITY.** Businesses are moving away from the "bunker mentality" that encouraged them to retreat behind so-called "hardened endpoints." Instead of aiming for a security standard that is impossible to achieve, they should focus on balancing resilience with productivity.
- **ORGANIZATIONS CAN IMPROVE RESILIENCE BY IMPROVING THEIR CRITICAL DATA CENTERS** and by making access to their systems more secure. Virtualization strategies and off-premise cloud architectures enable these data centers to be more secure than ever. Resilience should be about making data continuously available to those who should have access to it, and invisible to those who do not.
- **A TRULY RESILIENT ENTERPRISE DYNAMICALLY INNOVATES AND CHANGES ITS PRACTICES, POLICIES, AND PROCESSES,** in response to changing threats from the outside and changing requirements from the inside. Organizations must accept that data are protected by people, not machines. To improve resilience, they must enable and educate their workforce. ••

Worldwide Internet Penetration

70%

OF HOUSEHOLDS
ARE ONLINE

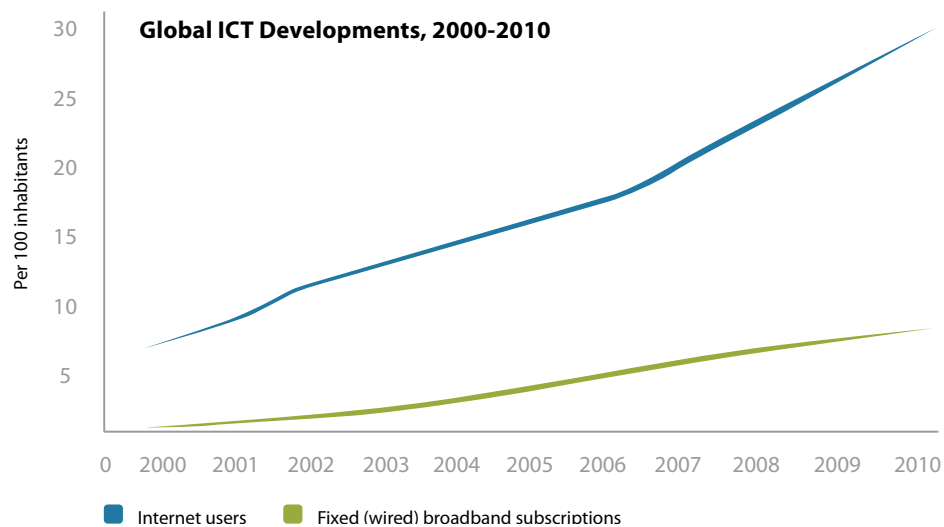
94%

OF BUSINESSES WITH
10 OR MORE EMPLOYEES
ARE ONLINE

Introduction

THE INTERNET HAS PENETRATED almost every corner of human activity. Among members of the Organization for Economic Co-operation and Development (OECD), 70 percent of households and 94 percent of businesses with 10 or more employees are online. Worldwide, the number of Internet users is projected to rise from 6.4 per 100 inhabitants in 2000 to 29.7 per 100 by 2010.

FIGURE 1 Ever-rising Internet penetration



Source: ITU World Telecommunication/ICT Indicators database

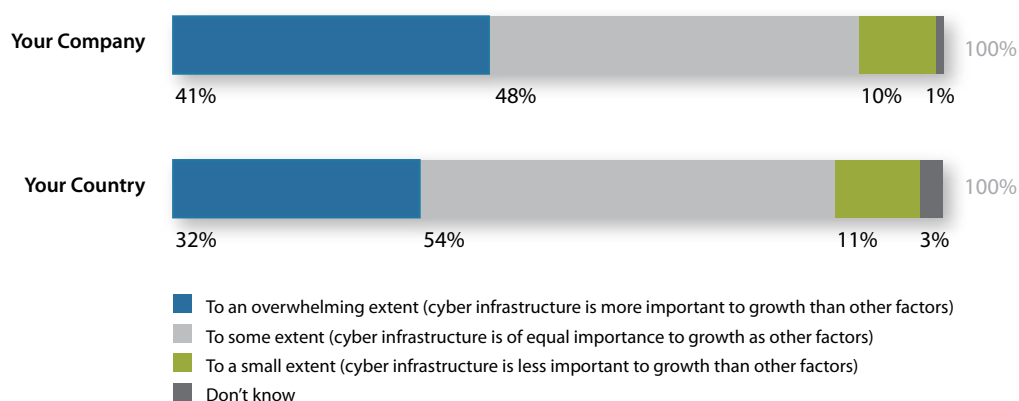
But as the world's digital market expands, so do the threats to its security. The estimated median cost of cyber crime for an organization—including loss of property, loss of productivity, and cost to remediate—rose from US\$3.8 million in 2010 to US\$5.9 million in 2011, according to Ponemon Institute's Second Annual Cost of Cyber Crime Study (2011). The number of cyber attacks has also increased by 44 percent per year, to an average of 1.4 successful attacks per week, per organization.

A survey conducted for this research program has confirmed the Internet's benefits and its risks.

One-third (32 percent) of executives say their country's economy relies on cyber infrastructure to an overwhelming extent. A further 54 percent say cyber infrastructure is at least of equal importance to their country's growth as other factors. When executives were asked the same question with respect to the economic growth of their organizations, 41 percent of respondents consider cyber infrastructure more important to their organization's growth than other factors, and 48 percent consider it of equal importance.



FIGURE 2 To what extent does the economic performance of your organization and the country where you are located rely on cyber infrastructure?



Source: Economist Intelligence Unit survey, July 2011

While the threats to cybersecurity for the world's businesses remain serious—and evolving, businesses are moving away from the “bunker mentality” that encouraged them to retreat behind so-called “hardened endpoints”. Web-based applications, mobile devices, and cloud infrastructures are changing the business and technology landscape simultaneously. A truly

resilient enterprise dynamically innovates and changes its practices, policies, and processes, in response to changing threats from the outside and changing requirements from the inside. Educating its workforce about the nature and function of these changes is one of the key paths to greater resiliency.

“The number of cyber attacks has also increased by 44 percent per year, to an average of 1.4 successful attacks per week, per organization.”

Resilience: Definitions Matter

NIGEL INKSTER, DIRECTOR of Transnational Threats and Political Risk at the International Institute for Strategic Studies, offers a scientific definition of cyber resilience: “the ability of a system or domain to withstand attacks or failures, and in such events, to reestablish itself quickly.”

But other definitions of resilience vary widely. In 2010, the US Department of Homeland Security commissioned a study on how institutions were implementing resilience principles. Its analysts came up with 119 different definitions, and concluded that a broader, more cohesive definition of resilience should include flexibility and adaptability.

Professor James P. G. Sterbenz, from the Communications and Networking Systems Laboratory at Kansas University, has been working on clarifying the concept of resilience for governments and organizations. The principles he and his colleagues have developed as part of the university’s ResiliNets data network architecture project have been adopted by the European Union’s government security agency, ENISA, and are in the process of becoming adopted by the US Department of Homeland Security.

Professor Sterbenz points out that notions of resilience can include several concepts that mean different things to different people. “Reliability and availability are very different,” he explains. “A reliable system is one that operates for a specified period of time, and you say what the probability is. Availability, on the other hand, is the probability that something will be there when you need it.”

Resilience means something entirely different to companies that are closely integrated into a nation’s critical infrastructure—be it the stock market, electric rail networks, or nuclear power stations. “We talk to our customers about what we call continuous service delivery,” says Garry Sidaway, Director of Security Strategy for Integralis, a global security consulting firm. “Whilst components might fail or you might have an incident, it’s about ensuring that service is still being delivered and the integrity of that service is still there.”

The new attitude in achieving resilience is to plan for acceptable levels of data loss, unit failures, and compromise. This may seem alien to executives who have historically maintained a “zero-tolerance” policy toward failures. But new cloud hardware architectures are demonstrating that everyday events like storage device failures and data loss can be tolerated when redundancies are built into the system.

The US Department of Homeland Security concluded in recent studies that “zero-tolerance” policies led to the perception that every unit of the business, whether digital or human, was critically important. When everything is critical, nothing is critical. When organizations enact more flexible tolerance principles, failures that would have shut down processes or even entire networks in an earlier era, won’t even be noticed by customers.

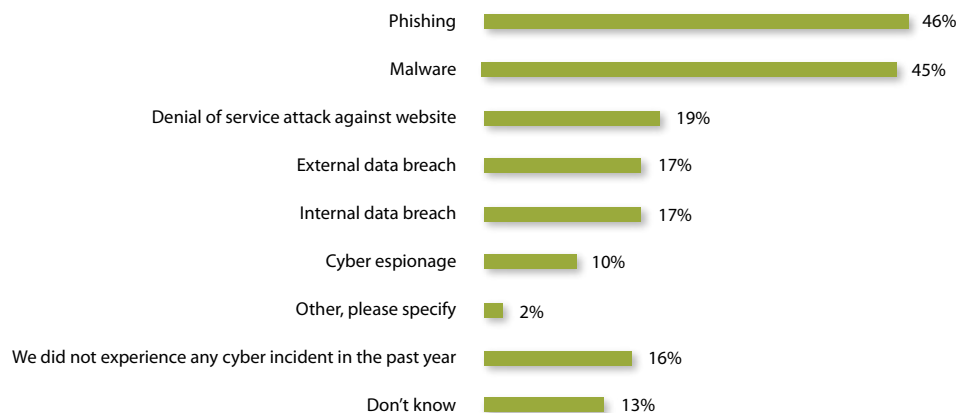
The Proliferating Threat

THE CYBER THREAT HAS EVOLVED from hackers functioning as hobbyists to something more serious and organized. Today's malicious agents are members of a growing industry of companies designed to infiltrate data centers to capture private information. Their primary strategy is to induce unsuspecting users to install malware on their PCs. Once installed, the malware converts the PCs into inadvertent attackers of the agents' final targets—data centers at Amazon, Rackspace, and elsewhere. In the summer of 2011, a number of security providers, including UK-based security services provider Webroot and other members of the Cloud Security Alliance, produced reports on these malware attacks. More instances of malware-based attacks were reported in the 18 months

leading up to these reports than in the preceding 18 years combined.

"From a risk management point of view, there's a whole new set of variables that have to be considered," says Mike Shinn, CEO of US-based Prometheus Global, a security consulting firm whose clients have included the White House and US Department of Defense (DoD). "There's a fairly widespread increase in economically directed criminal activity [for] the theft of intellectual property. Cyber criminals are now targeting everything from client lists, internal strategy documents, designs—everything up to and including information held by governments that would be of economic value."

FIGURE 3 What type(s) of cyber incident(s) has your organization experienced in the past year? Select all that apply.



Source: Economist Intelligence Unit survey, July 2011



The Corporate Response

THE INITIAL CORPORATE RESPONSES to cyber attacks have failed to address deficiencies in network architectures that allow the latest cyber attacks to occur. Ernie Rakaczky, Principal Security Architect with Invensys' process automation group, believes that companies' efforts throughout the last decade have led businesses to adopt a "fortress mentality" to protect their infrastructure. Although setting up firewalls and zones, policies, and procedures makes sense, they should not be done in a "reactionary mode," Rakaczky says.

The survey paints a mixed picture of the current state of corporate cybersecurity strategies. Some 53% of our survey respondents say their organization has a cybersecurity strategy already in place. Thirty-three percent of respondents admit they have no cyber-resilience strategy in place, and 14 percent were unsure. When asked to check three of the biggest barriers to their companies developing cybersecurity initiatives, among a list of nine, 41 percent of respondents cite lack of knowledge of the threat as holding back their companies.

Linda Laun, Global Consulting Portfolio and Methods Manager for IBM's Business Continuity and Resiliency Services team, notes that companies tend to focus on event-driven issues, things that are huge in scope—such as natural disasters, pandemics, power failures, and civil unrest—as triggers for invoking security measures. Laun believes that most companies know how to approach risks associated with security and data issues such as data loss or corruption, viruses, and worms, but she says they still struggle when dealing with risks associated with business issues like governance, compliance, audits, scalability, and performance.

Laun believes the problem is that responsibilities for these other security issues are confined within organizational silos. IBM advocates what it calls a Business Resiliency Management Framework (BRF) to distribute responsibility across multiple business units. The goal is to establish a centralized governance structure that allows stakeholders within the silos to set the direction of the program together through policy, measure success, and then "enforce" its policies.

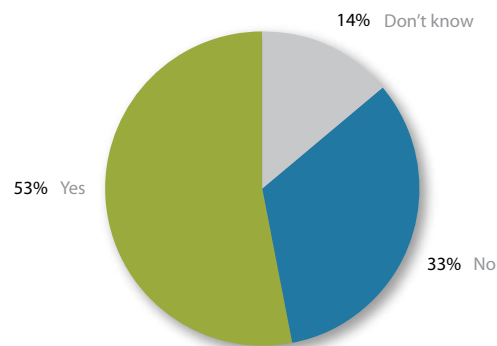
When asked to check three of the biggest barriers to their companies developing cybersecurity initiatives



The new attitude toward resilience accepts that companies cannot achieve perfect security or absolute continuity. Instead of aiming for a security standard that is impossible to achieve, they should focus on balancing resilience with productivity. "It is all about enablement," proclaims Integralis' Garry Sidaway. Instead of being seen as forces that say "No," he believes IT departments should ask how they can enable their company's employees to

be more productive no matter where they are or what devices they are using. "Whether it's working regular hours or out-of-hours, whether it's on a personal device or business device, how do we enable them to work and be productive in their jobs? That is the change in information security that we've got to drive towards, and we have a great opportunity to do that."

FIGURE 4 Does your organization have a cybersecurity strategy?



Source: Economist Intelligence Unit survey, July 2011

"Whether it's working regular hours or out-of-hours, whether it's on a personal device or business device, how do we enable them to work and be productive in their jobs? That is the change in information security that we've got to drive towards, and we have a great opportunity to do that."

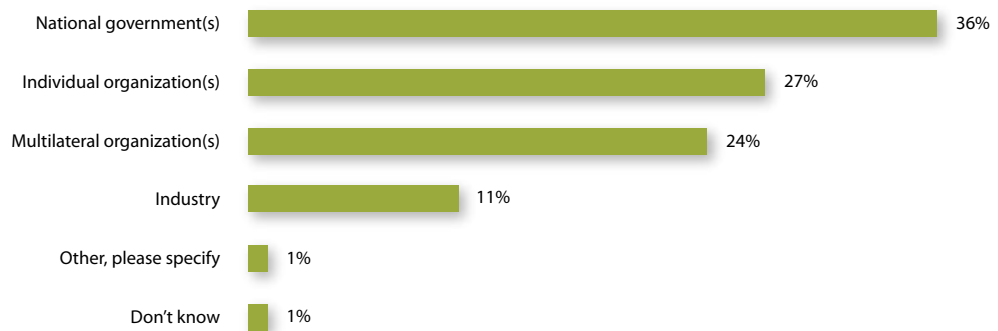
The Government Response

ALL AROUND THE WORLD, governments are expected to provide the leadership role for cybersecurity and resilience—a topic they are only just beginning to address. Executives believe their organizations and their governments could devote more resources to security issues. Approximately 67 percent say their organization needs to pay more attention to cyber risks, and less than one-quarter (23 percent) think their government is doing enough to promote cyber resilience. When asked whether they believed their country could do more to promote resilience, 57 percent of respondents said they think their governments could improve communication and awareness of cybersecurity issues; 60 percent

think governments could encourage greater cooperation between public and private sectors; and 56 percent think governments could promote technology innovation through programs such as cyber competitions.

Although 87 percent of respondents believe improved understanding should come from a greater partnership between government and private industry, a far lesser number (36 percent) believe government should actually take the leadership role in maintaining cyber security. In short, businesses want help, and they want it from government. But they do not want government to take control of the issue.

FIGURE 5 In your opinion, who is primarily responsible for maintaining cybersecurity?



Source: Economist Intelligence Unit survey, July 2011

The Role of Public/ Private Partnerships

DESPITE THE MODEST SUCCESS OF PUBLIC/PRIVATE PARTNERSHIPS (PPP) TO DATE, executives see some value in promoting collaboration. Eighty-seven percent of survey respondents agree that cyber resilience relies on some form of partnership between government, civil society, and business.

DARPA, the (DoD) agency tasked with technological innovation, offers a successful example of how to stimulate private sector innovation for the greater good. The agency assembles teams of experts who pursue innovative ideas. Little money is lost if they are unsuccessful, while successful projects are picked up by the private sector. One such case was ARPANET, the precursor to today's Internet. Among more recent examples are the DARPA Grand Challenges, a cash prize competition last held in 2007 that stimulated the development of driverless vehicles.

More recently, the DoD rolled out the Defense Industrial Base (DIB), a PPP initiative designed to share cyber threat information among organizations that support the US defense industry. In August 2011, the trial was pronounced successful, and the initiative is now being extended to include certain critical infrastructures.

The U.S. Cyber Challenge offers yet another model of public/private partnership. Karen Evans, the organization's national director, said she first got involved in the U.S. Cyber Challenge, "to test the hypothesis that you could hold an online competition and identify talent." The U.S. Cyber Challenge holds numerous competitions and events throughout the year and now also hosts a summer camp program, which in 2011 received 1,000 registrants for 200 available slots. Evans and her colleagues seek to harness the competitive nature of Americans and, in the process, identify highly talented individuals. The goal is to use the competition to eventually get 10,000 very skilled people to enter the workforce, taking modern resilience principles with them. ♦♦

Critical Infrastructure Issues: Developing Better System Architectures

THE FIRST WAY TO IMPROVE RESILIENCE is to improve an organization's critical infrastructure—its data center. Newer infrastructures enable these data centers to be more secure than ever, primarily because fault tolerance, replication, and workload balancing are all built into newer operating systems and newer hardware. These new structures are more effective than the "endpoint" hardening approach to system security, which focused on hardening security at PCs, smartphones, and other endpoint devices.

Dave Scott, the head of NTT Europe's Solution Consulting team admits that, although he was once an advocate of that approach, the precautions he took weren't enough. "I may have been naïve until my first data center outage," Scott says, "at which point, I wised up quite quickly. You can put together what you think are the best security endpoints and resilience within a single facility, and something will still happen that takes the whole thing out. You assume then that true resilience and true availability mean more than just endpoint security."

To improve security at data centers, it is necessary to address the three classes of operations they involve: processing (the execution of programs and the production of data, often called "compute power" by service providers); storage (the containment of data); and interconnect (the transmission of data and functionality). In an

earlier era, the processor was a central processing unit (CPU), the storage amounted to a couple of hard disk drives, and interconnect was managed through Ethernet cables.

Two new factors have changed the way data centers are managed. First, companies often employ virtualization strategies to improve compute power and storage in their data centers. A vast array of storage devices—on- and off-premise and clusters of processors—are made to appear to the operating system as a single pool of storage and a single processing engine. These pools are then “connected” to the network by way of software that simulates a physical network adapter. The result is a virtual machine whose size and location can be changed while it is still running.

Companies may also move part or all of their infrastructure off-premise via the cloud.

Organizations may use a hosted provider such as Rackspace for their servers, or a cloud service provider (CSP) such as Rackspace, Amazon, GoGrid, or BlueLock to host all or part of their data center at various times. This allows them to lease more compute power during peak usage times as well as other efficiencies.

Len Padilla, Senior Director of Technology for NTT Europe, believes that cloud architecture allows more companies to build failure and fault tolerance into their data architecture. Companies now have new ways to make their systems geographically blind and ramp up resources to address a load in a particular way. “That’s something that very big organizations with very big IT budgets have always been able to do, but now cloud computing allows even smaller and medium companies to do the same thing,” explains Padilla.

Application Issues: Resilience Through Better Software

ANOTHER WAY TO IMPROVE RESILIENCE

is through more modern applications. Newer software can be better managed than older software. However, too many organizations rely on work processes geared around old and even outmoded applications. For example, law firms institute chains of custody around their document-handling processes that presume that documents are transferred from person to person. Newer collaboration software that allows documents to

be used across a firm with auditing and versioning services are far more concrete and trustworthy. Similarly, many company employees send sensitive documents as attachments to one another via e-mail and institute security measures for ensuring encryption and validating receipts. A better alternative is to create shared storage spaces where only permitted individuals may be made aware of a document’s existence.

Invensys' Rakaczky explains that he still works with customers who use software and methods that date back to the turn of the century. In some cases, he has had to employ virtualization just to enable old systems to work on current hardware. He says that his customers often resist migrating to newer, more secure operating systems because they are restricted by notions of 3-year or 5-year software refresh cycles. If businesses try to upgrade

software before the end of a cycle, the cost often gets counted as a budget overrun.

Instead, Rakaczky tries to help his customers keep their systems in more of a continually concurrent state to make it easier to adapt to newer platforms. Planned, deliberate, and slow migrations distributed throughout the lifecycle of a software product can be more efficient than a 5-year overhaul.

Access Issues: Greater Availability by Focusing on Data

BUSINESSES CAN ALSO IMPROVE RESILIENCE by making access to their systems more secure. Existing networks often use a variety of different security measures. Internet connections are secured with firewalls. Mobile users are secured with virtual private networks. Data is secured with encryption. Sidaway believes these disparate "bolt-on" security technologies have created an overly complex environment that is difficult to manage. "We need to start thinking in terms of everything we need to do to enable our consumer to access that information in a secure way, and work productively in a secure environment that's easy to use," he says.

Now, Sidaway believes, we've arrived at a sensible model: A company's core asset to be protected is its data—not its servers or its firewall, or a dotted-line perimeter in the sand. Resilience should be about making data continuously available to those who should have access to it, and invisible to those who do not. He believes modern data centers must be designed from the top down without arbitrary compartmentalization. To increase resilience, businesses need to change their mindset from securing devices to securing data.

Workforce Issues: Becoming Resilience-Aware

Organizations must also accept that data are protected by people, not machines. To improve resilience, they must enable and educate their workforce. But few companies seem to be aware of this requirement. Less than one-third of survey respondents from companies that have a cybersecurity plan say employees are important stakeholders; in companies without a plan, even fewer recognize the importance of employees.

Padilla has thoroughly documented his company's resilience principles to help educate his workforce. At his company, a power outage, or a strike affecting the subway system, or a severe thunderstorm becomes an opportunity that allows the workforce to train for a more critical situation.

What NTT learns from these drills it then documents, with results that can then be shared with its own customers.

NTT collects a list of mistakes made during everyday work and emergency response. IT workforce members assigned to security then make it a point to communicate directly, person-to-person—not via e-mail or voice mail or Twitter. Next, the IT department follows up to make certain employees are following those best practices as directed.

Sidaway points out that information security policies need to be acceptable to the people who will carry them out. "If they're not acceptable to the employee, people will start working around it. You've got to get that balance right, so you can enforce it with technology. That becomes the part we have to monitor against compliance. Once you architect security into the system with technology, you've got to monitor that. But there's also that human element that comes into play, and it's often ignored when organizations look at risk and information security. It's people."



The Number of Cyber Attacks Has Increased...



The Industry Differences

THE PERCEPTIONS OF THE CHALLENGES AND OPPORTUNITIES OF A CYBER ECONOMY differ by industry. In a survey conducted by the Economist Intelligence Unit in June and July 2011, for example, 53 percent of respondents from financial services say that their industry relies on cyber infrastructure to an overwhelming extent, compared with 36 percent for the entire survey sample. Forty-seven percent of them also say their industry is more susceptible to cyber threats than their country or organization, compared with 23 percent overall.

Respondents from the energy sector tend to see the greatest risk at the national level, perhaps because energy systems—whether electric power networks or supplies of oil and gas—frequently have national security implications. Invensys manages such networks in real time and, therefore, cannot afford to utilize public cloud resources precisely because those resources lie outside of Invensys' direct control, says Rakaczky. But it can utilize technologies internally such as virtualization (the principal ingredient of cloud architectures) to enable greater direct control, and more avenues for fault tolerance and response to failures.

Invensys designs its networks to literally calculate resilience in real time—for example, maintaining the status of oil refineries with assets throughout North America, and registering the capacity and flow of fuel through every segment of pipe. According to Rakaczky, private cloud architectures can actually help Invensys utilize its data centers' processor power more efficiently, increasing the reliability of the real-time data it perceives. They can also distribute those data over systems in such a way that loss of data from one file—which will happen—does not and cannot destroy any single database.

"A power company will buy one of our systems and deploy it across its generation stations, controlling maybe five turbines generating a couple of hundred megawatts of power for a whole network of the grid in the United States," he explains. For those clients, security has always been provided by people, whether they are IT professionals or armed guards. So it only makes sense that performance, reliability, agility, confidentiality, and other resilience factors are managed directly by designated, responsible people as well.

Not every industry requires a level of sensitivity to real-time data as Invensys' clients. But the resilience principles it has pioneered can apply just as easily to a financial services provider, for example, as it does to a continental power grid. ••

A Newton's cradle with several silver spheres hanging from thin wires. The spheres are arranged in a diagonal line from the top left towards the bottom center. The background is a light blue gradient with a subtle grid pattern.

Conclusion

THE CYBER THREATS FACING COMPANIES HAVE CERTAINLY INCREASED, but they have been met by a host of powerful new ways to respond to them. Virtualization and cloud strategies now allow large and small companies to manage their data architecture with a flexibility that was impossible a few years ago. New collaboration software allows them to share documents more reliably on secure storage spaces. Modern data centers allow them to make their data continuously available to those who should have access to it, and invisible to those who don't. A well-trained workforce familiar with cybersecurity issues can help companies train for emergencies, respond effectively, and learn from their experiences. A truly resilient enterprise dynamically innovates and changes its practices, policies, and processes, in response to changing threats from the outside and changing requirements from the inside.

Resilience is achievable, but companies will have to change the way they operate to reach their goals. Resilient companies are stronger companies. By facing the resilience challenge, businesses can give their customers the trustworthiness and reliability they expect and deserve.

About Booz Allen Hamilton

BOOZ ALLEN HAMILTON IS A LEADING PROVIDER of management and technology consulting services to the US government in defense, intelligence, and civil markets, and to major corporations, institutions, and not-for-profit organizations. Booz Allen is headquartered in McLean, Virginia, employs more than 25,000 people, and had revenue of \$5.59 billion for the 12 months ended March 31, 2011.

Booz Allen understands that cybersecurity is no longer just about protecting assets. It's about enabling organizations to take full advantage of the vast opportunities that the ecosystem of cyberspace now offers for business, government and virtually every aspect of our society.

Those opportunities can be imperiled, however, by rapidly emerging cyber threats from hackers (hacktivists), organized crime, nation states and terrorists. We help our clients in both business and government understand the full spectrum of threats and system vulnerabilities, and address them effectively and efficiently.

Booz Allen believes the key to cybersecurity today is integration – creating a framework that “thinks bigger” than technology to encompass policy, operations, people and management as well. Through such a Mission Integration Framework, organizations can align these essential areas to address the real issues, and develop cyber strategies and solutions that keep pace with a fast-changing world.

To learn more, visit www.boozallen.com. (NYSE: BAH)

About the Economist Intelligence Unit

THE ECONOMIST INTELLIGENCE UNIT IS PART OF THE ECONOMIST GROUP, the leading source of analysis on international business and world affairs. Founded in 1946 as an in-house research unit for The Economist newspaper, we deliver business intelligence, forecasting and advice to over 1.5m decision-makers from the world's leading companies, financial institutions, governments and universities. Our analysts are known for the rigour, accuracy and consistency of their analysis and forecasts, and their commitment to objectivity, clarity and timeliness.



Booz | Allen | Hamilton

Economist Intelligence Unit

The
Economist

*An Economist Intelligence Unit
research program sponsored by
Booz Allen Hamilton*