IBM Center for Applied Insights

SecurityIntelligence

Executive Series

Security Essentials for CIOs

Embracing Innovation with Confidence

Every day, new streams of information flow into corporations, powering up-to-the-minute analysis and smarter decisions. Employees, customers and contractors are all connected as never before, across a multitude of technologies. Yet these sprawling and overlapping networks pose daunting security challenges. The complexity is dizzying, the possible points of attack near limitless. CIOs are grappling with growing frustrations—and questions. Is strong security even possible in a hyper-connected era? The answer is yes, but it requires fundamental changes in processes and attitudes. IBM has implemented its own strategy in-house and has mapped out the ten essentials required to achieve security intelligence in the 21st Century.

As the sun rises in New York, the VP for sales rolls out of bed, flips on her smart phone and sees that a big opportunity has surfaced in Malaysia. This news sets off a cascade of communication. Before breakfast, six members of the global team are on a teleconference, one of them through a Skype connection in Stockholm. Three contractors call in on cell phones. Throughout the day, e-mails crisscross the globe, about half of them on the corporate network, others on Gmail and Yahoo. By evening in New York, the deal is closed. In the following hours, a few of the participants friend each other on LinkedIn.

91%

of enterprise smart phone users connect to corporate e-mail, but only one in three is required to install mobile security software.

Source: Kaspersky Labs
http://usa.kaspersky.com/sites/usa.kaspersky.com/files/Enterprise%20Mobile%20Survey.pdf

It's no secret that managers today can summon brainpower and gigabytes of data in an instant, and use them to make faster and far better informed decisions. Yet the very strengths of these interconnected networks—their speed and openness, the easy access anywhere on the globe—also create a myriad of vulnerabilities. And the job of securing a corporation's network grows infinitely more complex as information pours in from thousands of devices and through scores of public Web-based services. A study by Kaspersky Labs reports that 91% of enterprise smart phone users connect to corporate email, but only one in three is required to install mobile security software. In such an environment, access is easy for everyone involved—all too often including criminal organizations.

Crime rings now regard Internet-connected PCs and mobile devices as prime real estate. By infecting devices with hard-to-detect malware, they extend their bases of operations. For thieves, corporate networks are bursting with digital treasures, including passwords, user IDs, business secrets, and personal information. Digital intruders also target strategic assets, from government ministries to communications networks. Some are out to disrupt business operations. Gartner's estimate is that 20 to 30 percent of consumer PCs have been compromised by botnets and malware that can be used as infrastructure for criminal operations. With many firms considering the enterprise use of personally-owned devices, the potential for infection is a very real concern.

20–30%

of consumer PCs are hosting malware, and working part-time for criminals.

Source: http://www.computerweekly.com/opinion/CW-Security-Think-Tank-How-to-prevent-security-breaches-from-personal-devices-in-the-workplace

A single infected computer can cause serious damage. One of the most dramatic examples to date is Stuxnet, a highly sophisticated worm engineered to cripple industrial software and equipment. In the spring of 2009, the worm began spreading through machines, most of them in Iran. Someone, it seemed, had introduced it through a contaminated thumb-drive. Developed to target machines running a Siemens software program, the worm wreaked havoc on numerous industrial systems.

The lessons for corporate security leaders is clear. If a worm can make its way into a heavily protected industries in Iran and elsewhere, how much easier would it be to find an opening in a globe-trotting work force of Twittering, Facebooking, texting and Skyping professionals. What's more, if a worm can disable industrial equipment, couldn't others shut down supply chains, reroute traffic, and damage electric grids, among other catastrophes? In a word, yes.

To face these growing challenges, corporations require **a new breed of security leader.** Naturally, they must be attuned to countless technology threats, but also to strategic issues. Which information should be shared broadly? Who should have access to certain jewels, and how will they be protected? Together, the technical and strategic challenges reach a dizzying complexity. And while the temptation may be to respond with solutions every bit as complex, far-sighted executives realize that such escalation is untenable, unaffordable and, ultimately, fruitless.

The only answer is to change, at a fundamental level, the way companies operate. It starts with **expanding the mission of enterprise security,** from the tech staff and their machines to every person within the company, and everyone who does business with it. This is only fitting: since each person poses a potential breach, each one must also represent a piece of the solution. In the end, success hinges upon creating a strong and persistent awareness: **a risk-aware culture.**

A risk-aware culture demands more than up-to-date technology and extends far beyond best practices. It represents a new way of thinking, one in which a pragmatic approach to security informs every decision and procedure at every level of the company. This must recast the way people handle information, from the C-suite to summer interns. In such a culture, secure procedures for data become second nature, much like fastening a seat belt or storing matches in a safe place.

It represents a new way of thinking, one in which a pragmatic approach to security informs every decision and procedure at every level of the company.

This is not a decision to postpone. Enterprise security is fast approaching a tipping point. Consider the elements. In the criminal class, professionals have taken over for amateurs. That drives up the threat. At the same time, companies have gained productivity and "empowered" workers by broadly distributing rivers of digital data on operations, marketing, sales and customer service. This multiplies vulnerability. And because the near totality of a company's business is now managed digitally, the consequences of a break-in can rock the entire firm. In sum: the thieves are more skilled, they have innumerable digital doors and windows to crawl through, and the stash inside is priceless.

While the stakes are sky high, the path to security can appear daunting—and confusing. While there is no lack of security products and services on the market today, our customers often tell us they are frustrated by a security market they perceive as lurching from headline to headline, seeking relevance in the latest security crisis or compliance dictates. Many don't know where to start or what to believe, often describing security and compliance as an investment with unquantifiable value, a dubious ROI, and all the appeal of speed bumps on a freeway. This confusion often leads to indecision–or worse, the decision to forgo innovation based on fear.

There's no getting around the fact that to secure an enterprise is a formidable undertaking, one that is never complete. What's more, changing a culture is hard. But this work is essential. Strong security is the cost of staying in business, and achieving it is within reach.

At IBM, we are constantly striving to find the balance between necessary innovation and the need to control risk. The company's comprehensive response includes technology, process and policy measures. It involves ten essential practices. Over the coming months, we will be distributing a series of white papers to walk you through them in greater detail. For now, here's a quick summary:

Our Security Essentials

1. Build a Risk-Aware Culture

The idea is elementary. Every single person can infect the enterprise, whether it's from clicking a dubious attachment or failing to install a security patch on a smart phone. So the effort to create a secure enterprise must include everyone. Building a risk-aware culture involves setting out the risks and goals, and spreading the word about them. But the important change is cultural. Think of the knee-jerk reaction—the horror—that many experience if they see a parent yammering on a cell phone while a child runs into the street. That same intolerance should exist, at a company level, when colleagues are careless about security. Management, of course, needs to push this change relentlessly from the very top down, while also implementing tools to track progress.

2. Manage Incidents and Respond

Say that two similar security incidents take place, one in Brazil, the other in Pittsburgh. They may be related. But without the security intelligence needed to link them, an important pattern—one that could indicate a potential incident—may go unnoticed. A company-wide effort to implement intelligent analytics and automated response capabilities is essential. Creating an automated and unified system will enable an enterprise to monitor its operations—and respond quickly.

3. Defend the Workplace

Cybercriminals are constantly probing for weaknesses. Each work station, laptop or smart phone provides a potential opening for malicious attacks. The settings on each device must not be left up to individuals or autonomous groups. They must all be subject to centralized management and enforcement. And the streams of data within an enterprise have to be classified, each one with its own risk profile and routed solely to its circle of users. Securing the work force means vanquishing chaos and replacing it with confidence.

4. Security by Design

Imagine if the auto companies manufactured their cars without seat belts or airbags, and then added them later, following scares or accidents. It would be both senseless and outrageously expensive. In much the same way, one of the biggest vulnerabilities in information systems—and wastes of money—comes from implementing services first, and then adding security on as an afterthought. The only solution is to build in security from beginning, and to carry out regular automated tests to track compliance. This also saves money. If it costs an extra $60 to build a security feature into an application, it may cost up to 100 times as much—$6,000—to add it later.

5. Keep it Clean

It happens all the time. People stick with old software programs because they know them, and they're comfortable. But managing updates on a hodgepodge of software can be next to impossible. Additionally, software companies sometimes stop making patches for old programs. Cyber criminals know this all too well. In a secure system, administrators can keep track of every program that's running, can be confident that it's current, and can have a comprehensive system in place to install updates and patches as they're released.

6. Control Network Access

Consider urban crime. Policing would be far easier if every vehicle in a city carried a unique radio tag and traveled only along a handful of thoroughfares, each of them lined with sensors. The same is true of data. Companies that channel registered data through monitored access points will have a far easier time spotting and isolating malware.

7. Security in the Clouds

Cloud computing promises enormous efficiencies. But it can come with some risk. If an enterprise is migrating certain IT services to a cloud computing, it will be in close quarters with lots of others—possibly including scam artists. In that sense, a cloud is like a hotel in which a certain percentage of the customers have bubonic plague. To thrive in this environment, guests must have the tools and procedures to isolate themselves from the others, and to monitor possible threats.

8. Patrol the Neighborhood

Say a contractor needs access to the system. How do you make sure she has the right passwords? Leave them on a notepad? Send them on a text message? Such improvising has risk. An enterprise's culture of security must extend beyond company walls, and establish best practices among its contractors and suppliers. This is a similar process to the drive for quality control a generation ago. And the logic is the same: security, like excellence, should be infused in the entire ecosystem. The ruinous effects of carelessness in one company can convulse entire sectors of society.

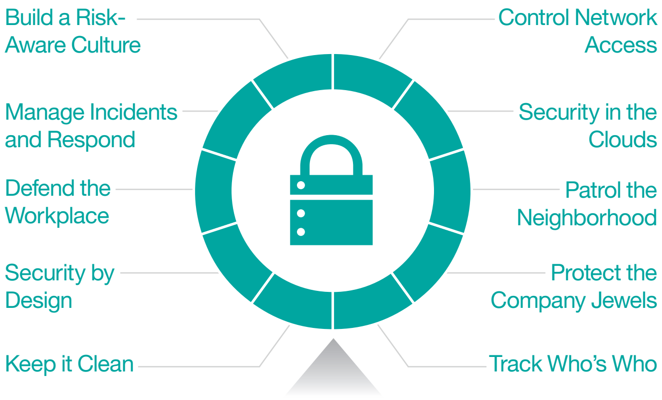
9. Protect the Company Jewels

Somewhere in the trove lie the company's critical jewels, perhaps its scientific and technical data, maybe some documents regarding possible mergers and acquisitions, or clients' non-public financial information. Each enterprise should carry out an inventory, with the critical data getting special treatment. Each priority item should be guarded, tracked, and encrypted as if the company's survival hinged on it. In some cases it may.

10. Track Who's Who

Say a contractor gets hired full time. Six months pass and she gets a promotion. A year later, a competitor swoops in and hires her. How does the system treat that person over time? It must first give her limited access to data, then opening more doors before finally cutting her off. This is managing the identity life cycle. It's vital. Companies that mismanage it are operating in the dark and could be vulnerable to intrusions. This risk can be addressed by implementing meticulous systems to identify the people, manage their permissions, and revoke them as soon as they depart.

How do I embrace innovation with confidence?



Balance managing risk and enabling innovation

Join the conversation

To read additional articles, learn more, or share your thoughts with other security leaders join us at **ibm.com/smarter/cai/security**.

About the author

Kristin Lovejoy is Vice President of IT Risk, Office of the CIO, IBM. She can be contacted at **klovejoy@us.ibm.com**.

About IBM Center for Applied Insights

The IBM Center for Applied Insights integrates deep content and analytical expertise to help chart the course to new value for clients. The Center conducts research and builds assets and tools with pragmatic guidance to provoke organizations to action.

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
January 2012