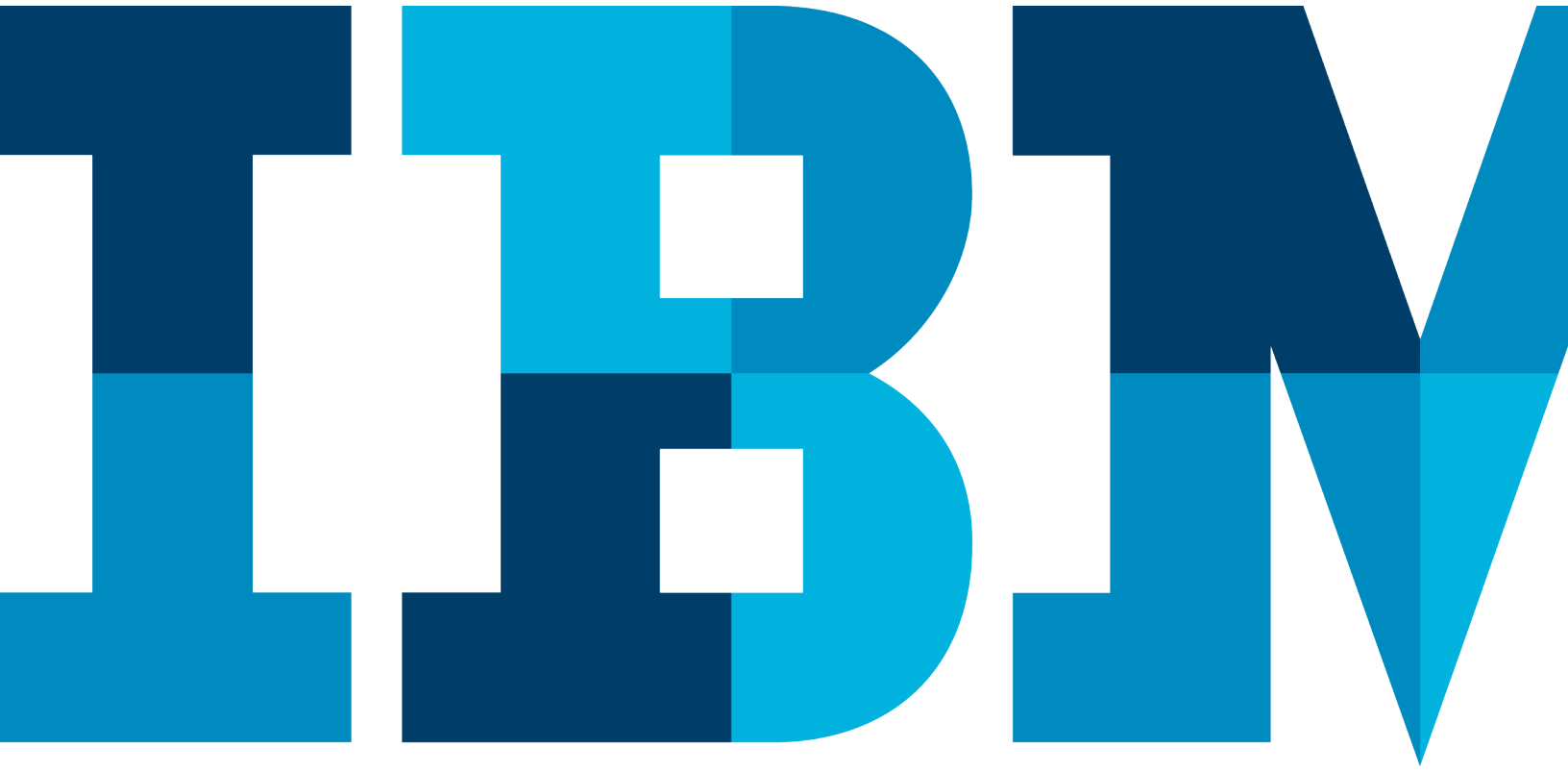
IBM Security
Thought Leadership White Paper

October 2014

Security principles for CEOs

Explore the five fundamental qualities of a risk-aware organization



Contents

Over the past several years, increasing numbers of companies, many of them household names, have revealed massive breaches of their computer systems— where attackers have stolen volumes of critical data and customer information. If anything, the low risks and high rewards of cybercrime have driven this to new heights. The frequency and impact of such attacks make security an executive and boardroom challenge.

How serious is the problem? The annual global cost of cybercrime is estimated to be more than USD400 billion, the national income of many countries.[1] In the US alone there were 1.5 million reported cyber attacks from mid-2012 through 2013.[2] Attackers' growing sophistication enabled them to steal more than a half billion records of personally identifiable information last year.[3] Such security breaches have also led to a 15 percent annual increase in the cost of dealing with a data breach—now totaling more than USD3.5 million per incident,[4] with damages related to the increased turnover of customers, reputation losses and diminished goodwill.

As a CEO, one of your fundamental responsibilities is to ensure that your business is secure. However, when it comes to cyber security, where should you focus? We suggest five action areas that are key to maintaining a strong security posture.

1. Increase the security IQ of every employee

You're only as strong as your weakest link. One study cites 60 percent of security incidents being caused by employee errors and internal system glitches.[4] Just having pockets of your organization doing the right thing isn't enough—it takes everyone to build and maintain a risk-aware culture. There will always be new threats and exposures—so education has to be continuous.

Workforce education—which should include your vendors, contractors and other third parties—needs to be conducted and tracked to help ensure that people are learning. You should also make testing part of your training program—both traditional quizzes to certify course completion and periodic organizational probes similar to the kind attackers themselves conduct.

Develop security policy and employee education

Problem: A European bank conglomerate sought to improve financial stability, reduce operational risk and enhance existing security programs.

Solution: IBM consultants established a consistent security policy in line with Basel II/III and helped create employee awareness programs.

Benefits:
- Reduced risk through a unified security program.
- Employees carry out security policies more effectively.

Consider, for example, conducting an enterprise-wide "spear-phishing" campaign—sending employees legitimate-looking emails with links that would take them to a theoretically "infected" site that could take over a computer's operating system and tunnel through to databases and critical assets. Find out who gets lured and who doesn't. Make it a teachable moment. At IBM, we've found that employees who've not yet completed security training are twice as likely to fall for an infected email as those who have.

To sum up, "train, test and trick" your workforce.

2. Prepare to respond, faster

Given recent headlines about cyber attacks on major companies, you need to assume a breach will occur. How you handle it is crucial, particularly the speed of your response. Sophisticated attacks often show no upfront "symptoms" but can quietly do devastating damage over a period of time. The longer it takes to resolve an attack, the more costly it becomes. Unfortunately, it has taken months for some companies to even become aware that they've been attacked.

Get a plan to guide your fast-response team

Problem: A major heart treatment center needed a response plan that also accounted for unique requirements such as the Health Insurance Portability and Accountability Act (HIPAA).

Solution: IBM consultants developed an incident-response plan for dealing with cyber-security incidents.

Benefits:
- **The center now has a blueprint for establishing a fast response to security incidents.**
- **Beyond dealing with the incident itself, the center now has a plan for working with all stakeholders affected by a security incident.**

Prevention, then, starts with an incident-response plan, mock exercises to test the plan and targeted efforts to proactively identify hidden malware and attacks already present in your infrastructure. You need to monitor what is happening across your infrastructure in order to have the necessary security data to help identify and defend against an attack.

You also need a fast-response team well versed not only in directly mitigating the breach but also in dealing with all aspects of a crisis. This is a core, year-round group drawn from such departments as IT, human resources, law, regulatory, sales and public relations that can deal with all the affected stakeholders in a security incident. This team should be trained and taken through periodic simulated attacks.

Bottom line: You must plan and practice responding to a cyber attack.

3. Safeguard BYOD—your employees are the new perimeter

It's clear that personal smartphones, tablets and other devices beyond standard workstations or laptops are all becoming tools of choice—so much so that many professionals use them on the job—even if they buy them themselves.

With such a proliferation of personal technology, you have to secure your organization in order for bring-your-own-device (BYOD) programs to work. This is where governance, policy and workforce education all come into play. The best technology solution available won't work if employees aren't educated and use policies aren't in place.

It's worth the time to define which uses are or aren't permissible and what the company will and won't do. As important, employees must be alerted to and made to comply with business conduct guidelines for the security of all.

Containerization—a way to isolate corporate data on personal devices—has become an important tool in BYOD, enabling the enterprise to safeguard critical information and employees to be confident the organization isn't accessing their personal information.

Reduce the risk of BYOD

Problem: A technology provider wanted more flexibility in its support of employee-owned devices. The existing policy blocked network access for any device type it had not previously examined and certified.

Solution: The company now uses MaaS360® from Fiberlink®, an IBM company, to identify, control and secure all mobile devices entering the enterprise, whether they're provided by the company or part of its BYOD program.

Benefits:
- **Strong security of corporate network and data.**
- **Increased employee satisfaction with a more flexible BYOD policy.**

4. Protect your crown jewels

Critical data—your "crown jewels"—are the small but most important portion of data vital to business survival and success. This includes proprietary data such as trade secrets, intellectual property, and confidential business plans and communications. While it's less than 2 percent of your overall data, it can represent as much as 70 percent of your market value.[5] Losing data costs money; losing the crown jewels can cost the business.

Many organizations, however, have no program to safeguard these most vital assets. As a CEO, you want to make sure your business does. Have your crown jewels been identified and classified? If so, where do they reside? On which devices or databases? Has your critical data been prioritized and assessed for risk of loss?

Protect your critical information

Problem: A government agency in the Middle East needed to discover and classify its most sensitive information. The agency also wanted to determine the data's value and apply adequate security controls to it.

Solution: IBM consultants worked with the agency to create a data security strategy and architecture to safeguard databases and critical information.

Benefits:
- **The agency's critical information has been located, analyzed and ranked for sensitivities and security vulnerabilities.**
- **The agency has a roadmap for safeguarding its critical data without inhibiting performance and availability.**

Once you've answered these questions, you want to identify and hold accountable those managers responsible for securing and protecting data. Because your crown jewels are so important, you should be prepared to apply considerable time and technology toward protecting them.

5. Leverage security intelligence

Storing and analyzing the mountain of data relevant to detect, let alone predict, a security event is a challenge. That data can include billions of events per day from traditional sources such as firewalls, emails and servers, as well as new areas like mobile users and cloud services. It's simply not possible to manually sift through this data and find evidence of suspicious behavior. Beyond the costs involved, it has confined enterprises to figuring out "what has happened" rather than "what will occur."

Big-data analytics tools are changing all this. Analytics applied to business data provide new insights and help drive transformation in the organization. When applied to security data, they can be just as transformative—the tip of the spear in security intelligence and response. Analytics can provide automated, real-time intelligence and situational awareness about your infrastructure's state of security to help disrupt the attack chain.

Use advanced monitoring and analytics to safeguard the organization

Problem: A South American bank needed to improve its security posture by integrating data from all its systems and applications.

Solution: IBM® Security QRadar® Log Manager and IBM Security QRadar SIEM help prevent advanced threats by implementing trusted protections and providing predictive analytics.

Benefits:
- **Superior threat detection and a richer view of enterprise activities.**
- **Sizable reduction in security events.**
- **99 percent decrease in investigation time.**
- **Immediate detection and notification of anomalies.**

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.

In conclusion, while there's no one-size-fits-all tool to maintain a strong security posture, there is one common action any CEO can take: communicate through words and actions that security is essential to the organization and that everyone has a role to play in it. To reiterate, executing on the five essentials that we recommend should be at the core of the organization's security strategy. By focusing on the basics, you can help safeguard your enterprise and enable it to move more nimbly—the difference between "getting it done" and "doing it securely."

Conclusion

IBM offers both deep experience in security and a long history of working effectively with clients—even in the most complex enterprise environments—making us uniquely qualified to help protect your brand and critical data. We provide unmatched global coverage and security awareness, with thousands of analysts and delivery specialists who provide security services every day for clients. IBM has 10 security research centers, 10 security operations centers and 15 security development laboratories. We also have more than 1,000 security patents. Additionally, we manage tens of thousands of security devices for thousands of clients worldwide. Our systems monitor 15 billion network events for our clients each day across 133 countries.

For more information

To learn more about IBM Security, please contact your IBM representative or IBM Business Partner, or visit:
ibm.com/security

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

Produced in the United States of America
October 2014

[1] Center for Strategic & International Studies, Intel, 2014.
[2] IBM Cyber Index Report, 2013.
[3] IBM X-Force® Threat Intelligence Quarterly, 1Q 2014.
[4] Cost of a Data Breach Study, 2014, Ponemon Institute.
[5] Commission of the Theft of American Intellectual Property Report, 2013.

Please Recycle

WGW03081-USEN-00