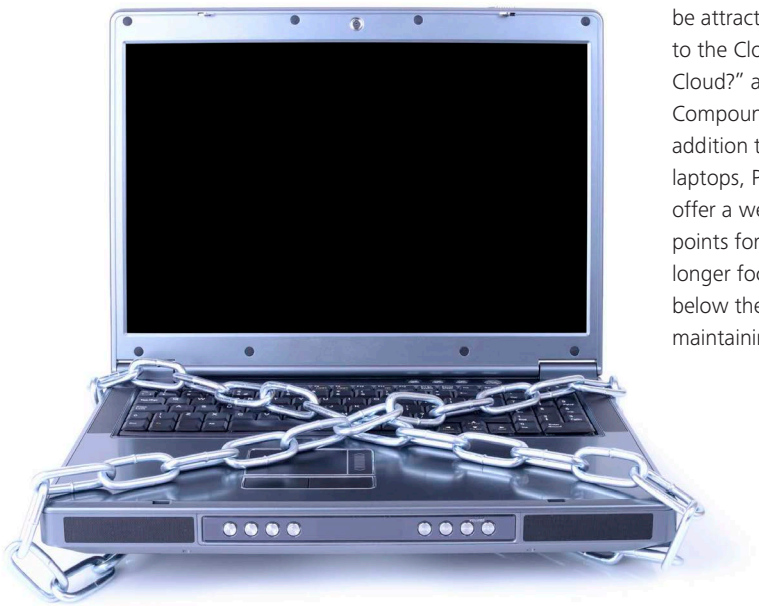
Deloitte.

CFO Insights
Cybersecurity: Five essential truths

Cyber risks, it seems, are everywhere. Retailers breached. Intellectual property stolen. Data hacked almost on a daily basis. It's enough to rattle even the most steadfast of chief financial officers (CFOs)—and often it does.

In fact, in our quarterly *CFO Signals*™ survey, cyber attacks have become a fixture on the list of CFOs' most worrisome risks, which includes perennial macroeconomic factors, such as economic volatility and overregulation.[1] In fact, four years ago when the survey first launched, cyber risk was rarely mentioned, whereas today it is routinely cited. And in our CFO Transition Lab™ sessions, newly named CFOs tell us of their increasing concern for cyber attacks.

That change in mind-set is directly correlated to both the frequency and the cost of cyber attacks. According to the Ponemon Institute's "2014 Cost of Breach: Global Analysis" study, the average total cost for a data breach is now $3.5 million globally, up 15% from last year (and considerably higher—$5.85 million—for U.S. companies).[2] In addition, the survey found that a company's probability of a material breach involving 10,000 records or more stands at 22% over the next 24 months.[3]



Given the costs and the increasingly malicious nature of the attacks, CFOs are understandably focused on identifying potential cyber risks and planning their corporate responses. Moreover, with a large percentage of finance chiefs also overseeing IT, they are equally committed to determining how and where to invest company resources on prevention. In this issue of *CFO Insights*, we will discuss some basic "truths" about cybersecurity and offer guidelines for investing in an enterprise-wide cybersecurity plan.

Fighting a moving—and evolving—target

For CFOs, getting a handle on cyber risk can be a frustrating process. Part of the problem is that finance chiefs typically don't have trend information on their companies' vulnerability. Plus, with the ubiquitous nature of cyber risk, classic security controls (firewalls, antivirus, Intrusion Detection Systems [IDS], Intrusion Prevention Systems [IPS], and so on) are increasingly less effective as attackers employ innovative techniques to evade them (see Deloitte LLP video: "Companies like yours"[4]).

Meanwhile, the battlefield keeps expanding. Consider the march to the Cloud. While the potential savings might be attractive, there's inherent security issues with going to the Cloud, such as "Who has access to my data in the Cloud?" and "Can it be shared with other customers?" Compounding the problem is the mobile evolution. In addition to standard desktop computers, company-issued laptops, PDAs, cell phones, and mobile phones typically offer a wealth of personal information and multiple access points for cyber thieves. Those thieves are also patient: no longer focused on "smash and grab," they are operating below the security radar of victim organizations and maintaining a presence for years.

What that means is that companies—and CFOs—are fighting a multifront, long-term battle where victory is difficult to measure. To have any chance of winning the cyber wars, however, there are several realities that CFOs should understand:

1. **Your information network will be compromised.** Unfortunately, it's inevitable that you will be attacked. If you operate an information network, you're not going to get to a point of zero risk. Accept it.

2. **Physical security and cybersecurity are increasingly linked.** Typically, the physical security domain and the cybersecurity domain have been viewed separately. But that is no longer the case. Why? While threats like espionage, intellectual property theft, fraud, counterfeiting, and terrorism may involve cyber breaches, they potentially can begin by physical access. In a common example, certain administrators may have full control over a system such as payroll, customer data, or billing. And armed with that access, those employees or contractors might pay themselves with false invoices, approve loans with special rates, or copy customer credit-card data and employee files containing sensitive information such as Social Security numbers, with the purpose of selling the data, creating identity theft, embezzlement, or other fraud.

3. **Cyber damages go beyond dollars.** While the average cost of a data breach may be well documented, the long-term effects on corporate reputation and brand significantly add to the toll. In particular, breaches of customer data can lead to a breakdown in trust that could inevitably hurt the top line—one reason several payment networks are demanding that retailers move to new payment cards that store information on computer chips rather than on traditional magnetic stripes.[5] In addition, many companies are now considering cyber insurance to limit excessive damages.

4. **Everything can't be protected equally.** Ask yourself, "What and where are the crown jewels in my organization?" In other words, what data is crucial to running the organization, and what databases, if compromised, could put you out of business? Not every piece of information, after all, is equally important. To a retailer, for example, customer credit-card data and employee Social Security numbers are crucial, as is logistics information related to supply chains. By making a hierarchy of data customized to your company and industry, however, CFOs can also make better decisions on how to prioritize protective controls and other aspects of cyber spend.

5. **Your walls are probably high enough.** Companies continue to invest heavily in the protection side of cybersecurity—more firewalls, more intrusion-detection systems. But most wall building may be about as high as it needs to be. Given that hackers have likely already infiltrated, companies should focus more on the detection side to increase their vigilance against attacks and on recovery after the fact. The formula is different for every company, of course, but of the typical IT cyber-risk spend, 30% might be allocated to wall building, 50% to detection, and another 20% to resilience preparation.

Figure 1. How cyber thieves attack

Incident classification pattern	Percentage
Point of sale system intrusions	14%
Web app attacks	35%
Insider misuse	8%
Physical theft/loss	<1%
Miscellaneous errors	2%
Crimeware	4%
Card skimmers	9%
Denial of service attacks	<1%
Cyber espionage	22%
Everything else	6%

Frequency of incident classification patterns from 1367 breaches during 2013.
Source: Verizon 2014 Data Breach Investigations Report

Tenets of effective cyber-risk programs

Accepting these "truths" is foundational to instituting an effective enterprise-wide cyber-risk plan. The action steps that can then be taken include the following:

Create a corporate-wide cyber mind-set. There has to be awareness, education, and training throughout the organization to combat cyber risk. You may have top-notch hardware and software to protect you against cyber intruders, but it might take only one unaware employee opening an attachment with malicious software to shut down your systems. The tone in combating this really does start at the top, with the board, CEO, and the CFO setting the governance and the organizational structure and making sure all employees are aware of their role in preventing cyber attacks.

Ask the right questions, of the right sources. As CFO, your go-to sources about cyber risk are typically the CIO, the chief risk officer (CRO), and the chief information security officer (CISO). The following questions can inform the dialogue:

- How do we identify our critical assets, associated risks, and vulnerabilities?
- Do we have a well-tested incident response and communication plan?
- Do we track what information is leaving our organization and where it is going?
- How do we know who's really logging into our network, and from where?
- Can we limit the information we voluntarily make available to a cyber adversary?
- Do our security controls cover the entire company, including subsidiaries and affiliates? (Most often the answer will be no.)

Cybersecurity checklist

There are steps you can take to reduce the threat of a cyber attack. In fact, according to the Ponemon Institute's "2014 Cost of Breach: Global Analysis" study, having a strong security posture, incident response plan, and chief information security officer appointment reduced the cost of a data breach by $14.14, $12.77, and $6.59, per record, respectively.[7] In addition, the following actions can guide CFOs in instituting an enterprise-wide cybersecurity plan:

1. **Evaluate the existing cyber-incident response plan.** Focus on the controls for the "crown jewels" and what you would do in the event of an incident. The team responsible for this should include senior management from the lines of businesses and administrative functions.

2. **Identify finance's role in cybersecurity.** Work with your CIO and the business leaders to see how finance can help create the necessary culture of security and privacy. Organizations can enhance their security stance by valuing cybersecurity and the protection of privacy and viewing. Remember: "Security begins with me."

3. **Require regular reports on security risks.** These reports should be from senior management and detail privacy and security risks, based not on project status but on specific risk indicators.

4. **Review the cybersecurity budget.** Many times, security budgets take a backseat to other IT or business priorities, resulting in companies being unprepared to deal with risks and attacks. An annual review of cybersecurity budgets is recommended.

5. **Reevaluate cyber insurance.** Also on an annual basis, revisit the use and need of cyber insurance.

Adopt a cybersecurity framework. In February, after a yearlong private-sector effort, the Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 was released by the National Institute of Standards and Technology.[6] A specific deliverable from the "Executive Order—Improving Critical Infrastructure Cybersecurity" that President Obama announced in his 2013 State of the Union address, the framework is intended to provide companies with a set of industry standards for managing cybersecurity risks. Voluntary in nature, it defines how to identify, protect, detect, respond, and recover from cyber threats, and the hope is that it will become a baseline leading practice for companies to use in, say, assessing legal exposure to cyber risks. The framework may impact your organization in several ways, including driving greater involvement by the board in overseeing cybersecurity risk and potentially requiring information-sharing protocols to be established. Lack of adoption, on the other hand, may lead to additional regulation for "critical infrastructure" sectors.

Designate an "Inspector General." One leading practice that some companies are employing is to shift the monitoring and investigation of cyber risk to an internal designee, whose role is like that of an Inspector General. That person is then charged with investigating a breach if it occurs and reporting out. The Inspector General does not own all of security, but can break the language barrier between cyber specialists and management. In some companies, for example, CIOs are charged with maintaining an adequate level of walls, but the monitoring or detection is done by someone in the CRO organization who reports up to the CFO.

Get educated. As CFO, you have to be educated on cyber risks and not rely solely on your CIO, CISO, or even the designated Inspector General. That doesn't mean simply taking an online course or reading one of the hundreds of cybersecurity books now in circulation. It means gaining hands-on exposure to cyber threats through modeling your business risks and then digging into the "what and how" of security.

Test the security plans. Cyber-simulation exercises allow participants to face off as the good guys and bad guys in real time, and offer a way to quickly get up to speed on the risks, identify where the organization's most important assets are, and pinpoint solutions for prevention.

Gaining a comfort level

Companies are under a continuous threat of cyber attack—a threat that cannot be ignored. By understanding these truths and instituting these action steps, CFOs may not gain complete comfort, but they may achieve a comfort level based on the protect-and-detect controls within their risk tolerance. The very nature of cybersecurity, after all, doesn't allow for a total solution. But, by instituting an enterprise-wide cyber plan, CFOs may at least achieve some measure of security.

Endnotes

[1] "What's Keeping CFOs Up in 2014?" *CFO Insights*, June 2014; *CFO Signals*, Q2 2014; U.S. CFO Program, Deloitte LLP.

[2] "2014 Cost of Data Breach Study: Global Analysis," Ponemon Institute, May 2014.

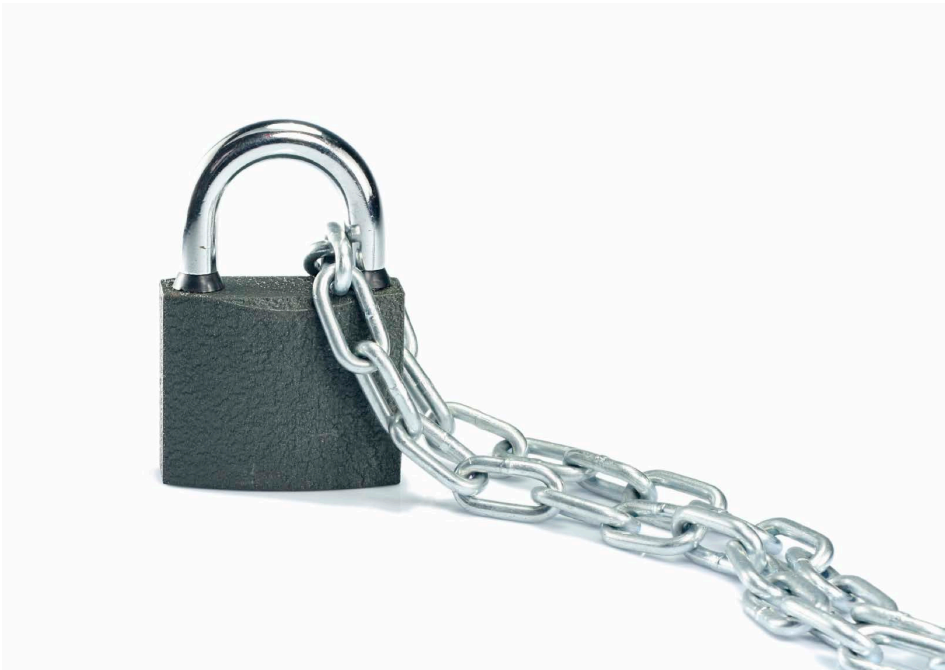
[3] "2014 Cost of Data Breach Study: Global Analysis," Ponemon Institute, May 2014.

[4] "Companies like yours," Deloitte LLP, 2011.

[5] "MasterCard, Visa and American Express Propose New Global Standard to Make Online and Mobile Shopping Simpler and Safer"; press release, October 1, 2013.

[6] Framework for Improving Critical Infrastructure Cybersecurity Version 1.0, National Institute of Standards and Technology, February 2014.

[7] "2014 Cost of Data Breach Study: Global Analysis," Ponemon Institute, May 2014.



Contacts

C. Kelly Bissell
Principal, Security and Privacy
Deloitte & Touche LLP
kbissell@deloitte.com

Harry Raduege, Lt. General, USAF (Ret.)
Senior Advisor & Director, Cyber Risk Services
Deloitte & Touche LLP
hraduege@deloitte.com

Deloitte *CFO Insights* are developed with the guidance of Dr. Ajit Kambil, Global Research Director, CFO Program, Deloitte LLP; and Lori Calabro, Senior Manager, CFO Education & Events, Deloitte LLP.

About Deloitte's CFO Program

The CFO Program brings together a multidisciplinary team of Deloitte leaders and subject matter specialists to help CFOs stay ahead in the face of growing challenges and demands. The Program harnesses our organization's broad capabilities to deliver forward thinking and fresh insights for every stage of a CFO's career – helping CFOs manage the complexities of their roles, tackle their company's most compelling challenges, and adapt to strategic shifts in the market.

For more information about Deloitte's CFO Program, visit our website at: www.deloitte.com/us/thecfoprogram.