Cyber-Security's Weakest Link: *People*

By Mike Mantzke, President and CEO

Global Data Sciences, Inc.
2112 W Galena Blvd., Suite 8246
Aurora, IL 60506
(630) 299-5196
www.globaldatasciences.com

Introduction

A stark reality facing today's businesses is the never-ending threat to cyber-security and a strategy for how to combat it. An even greater concern is damage to corporate image, consumer trust, loss of revenue, liability to customers, and the ever-increasing statutes imposed by lawmakers and agencies who point the finger at businesses for failure to take responsibility for preventing data theft.

Cyber-attacks are real and occur often in the places we shop, the materials we move throughout factories and nearly everything we take for granted. Incessant waves of computer, server, cloud and mobile hacking have led to compromised data, unwarranted access to private information such as Social Security numbers and bank accounts, and industrial espionage. The number of attacks on companies has become nearly unquantifiable. The Heritage Foundation reported that in 2015, "companies saw an average of 160 successful cyber-attacks per week, more than three times the 2010 average of 50 per week."[1] As early as 2006, Joe McGrath, at the time the president of Unisys, called the security of data and systems processes "an incredible challenge in the global/digital economy."[2] All these years later, this still is true. In fact, it's become worse.

Yet for inexplicable reasons, businesses give what is little more than lip service when it comes to cyber-security. They tend to overlook vulnerabilities even as the number of mobile devices such as smartphones and tablets that can access data worldwide increases. Too many companies allow employees and associates to access data from either corporate-owned or private devices away from the workplace. Such access, regardless of password protection and, in some cases encryption, is a chasm that provides a huge opening for cyber criminals who are all-too capable of penetrating servers through apps or other stealth measures.

Hackers remind us on a daily basis that no one is totally secure. In fact, it's a lesson that most businesses should have learned by now. Moreover, for all the emphasis on technology, the weakest link in cyber-security may go beyond technology and have everything to do with people, specifically those who manage and maintain the system. Failure to identify and correct human shortcomings is a flaw that can and most often will render a system vulnerable and likely to be exploited.

Why aren't businesses giving equal attention to the human element as well as the technological one? Perhaps it's because they are so focused on stopping external threats that they overlook weak spots in their first line of internal defense—their people.

Background

Because of successful foreign and domestic hacking, those in charge of cyber-security can no longer believe that their systems are invulnerable or that their firewalls, alert systems and best practices are sufficient to fend off would-be invaders. True, there are many tools designed to ensure system security such as sophisticated algorithmic encryption codes, but even those may not be as secure as one would want to believe if there are issues with those responsible for the system.

Businesses and other types of organizations need not look beyond the last few years to recognize how ubiquitous and pernicious security threats can be if they are not completely understood. In May 2016, the hack of Myspace may have compromised more than 300 million records. The hacker has reportedly put the data on a website for sale. Another example: China-based hackers, who are believed to be responsible for penetrating the U.S. Office of Personnel Management and "stealing addresses, health issues and financial details of 19.7 million people who had been subjected to background checks."[6] Then there is the infidelity-encouraging website Ashley Madison in which 11 million would-be scheming lovers had their credit card records and personal correspondence hacked AND publicized. *Information Age* identified the perpetrators as a "hacking collective" able to exploit flaws in the site's password encryption. Ashley Madison's share price immediately plummeted, and its legal counsel will no doubt have to deal with costly litigation from those who were, for all intents and purposes, busted.

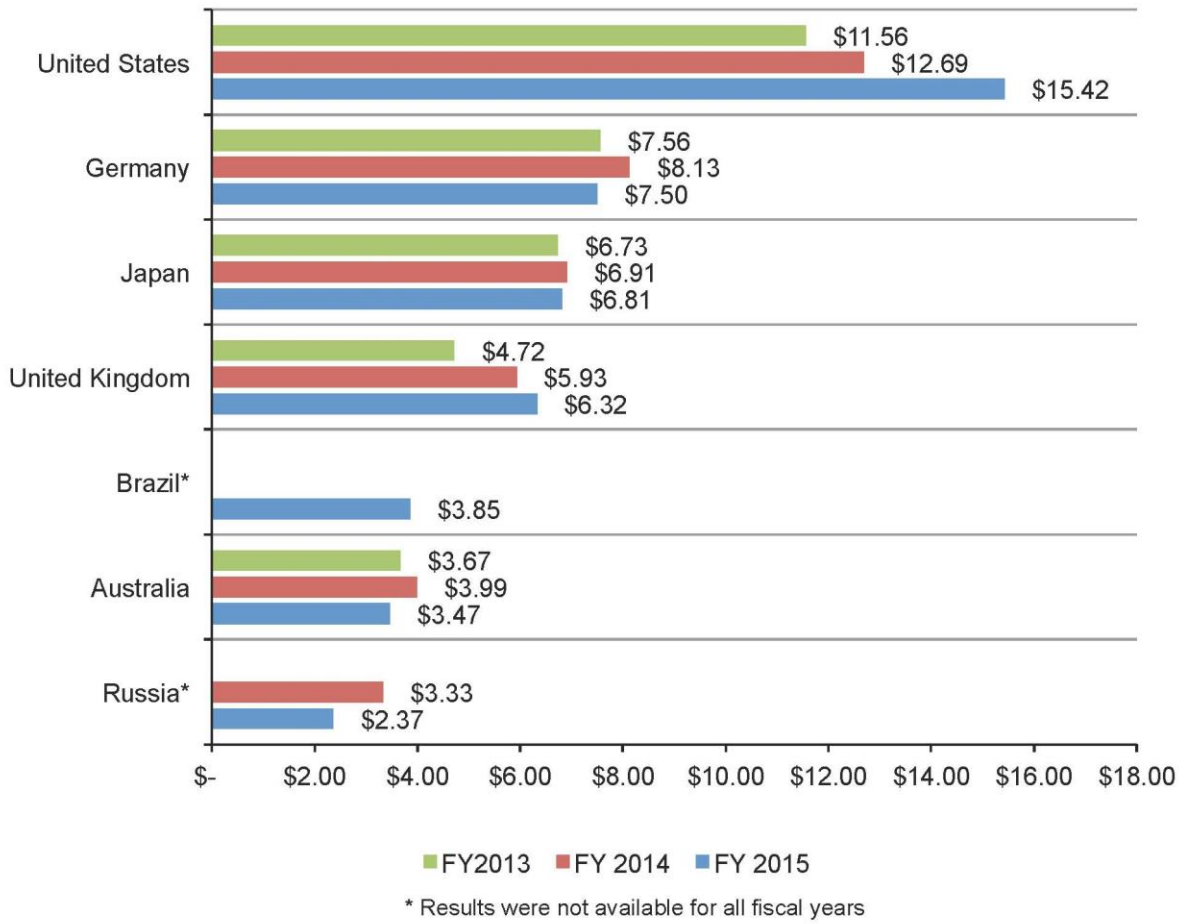
Add Experian to the list. The credit rating company's security could not stop hackers from stealing names, addresses and, worst of all, social security numbers of 15 million people. And in 2012, hackers penetrated the South Carolina Department of Revenue and managed to steal credit card and probably tax information of an estimated 3.6 million people. Had there been an encryption program in place, preferably more than one level, the data more likely would have been secure.

Organizations Affected by Cyber Attacks

myspace	Office of Personnel Management	Ashley Madison.com	Experian	South Carolina DOR Department of Revenue
300 million records compromised	19.7 million records compromised	11 million records compromised	15 million records compromised	3.6 million records compromised

In December 2015, *Information Age* also issued this warning to readers, "Whether the target is a massive corporation or a micro business, no organization is too big or too small to escape hackers' scrutiny."[3] The Ponemon Institute in its "2015 Cost of Cyber Crime" study found that the United States "continues to rank highest in its cost of cyber-crime at an annual average of $15.4 million per company."[4] According to the Heritage Foundation, the minimum cost was $1.9 million; the maximum—$65 million[5].

Total Cost of Cyber Crime in Seven Countries
Cost expressed in US dollars (000,000), n = 252 separate companies



"*2015 Cost of Cyber Crime Study: United States*." Ponemon Institute. Sponsored by Hewlett Packard Enterprise. October, 2015. Reprinted with permission.

It is important for those involved not to automatically dismiss the successful hacks to flaws in technology. What about those responsible for protecting these systems? Why were they unaware of the flaws that hackers somehow identified and exploited? This is a people question, and it is applicable to any and every entity with a database. Failure to recognize shortcomings in IT has to be recognized as a vulnerability that could and has jeopardized data protection.

The Importance of End-to-End Encryption

Many tools, when used properly, especially by the major carriers, will help companies detect and avert threats. Perhaps that explains why so many remain oblivious to possible underlying issues. That all-purpose popular repository—the cloud—is also vulnerable. In spite of its values in terms of cost, server and data efficiency, the servers that feed the cloud are equally subject to attack. Let's not forget point-of-purchase terminals. They have always been ripe targets for hackers who have not hesitated to take advantage of their shortcomings in a variety of ways. In recent years manufacturing and utility industries have become the objects of hacker penetration. Introduction of integrated shop floor machines used for data collection, analysis and controls often referred to as IOT (Internet of Things), Smart Manufacturing, Industry 4.0 among others, have proven to be highly desirable targets for corporate espionage or facility disruption.

Firewalls and monitoring systems are supposed to protect the data, but they sometimes fall short with disastrous consequences for the business or public entity. Why? Because once the firewalls are penetrated, the data can and will be stolen easily unless there is end-to-end encryption. In this case we're talking about protection for data in motion (emails, texts, etc.) or data at rest (sitting on a server disk).

This is another example of where IT cannot rest with just one level of encryption. Using an accepted encryption method such as AES 256 is good, but not good enough. IT should not be satisfied with just one level. The best approach is to add another level such as Bit Shifting to increase data protection. It takes the right people to aggressively manage and protect the system in this manner. In the end, everyone has to be accountable, including those above the IT team, all the way to the C-suite.

The U.S Securities and Exchange Commission is leading the way to force accountability at the executive level. The SEC cracked down on a St. Louis investment advisory firm because its failure to implement policies and procedures led to a breach that compromised personally identifiable

information of 100,000 persons."[7] Other governmental agencies are reported considering making C-suite people accountable for security breaches.

The message here is that people at all levels are responsible for getting it right.

Cyber-Security Policy: Lessons Learned

An intense focus on infrastructure should not diminish the necessity of protecting raw data and keeping it safe. To do that, every company or organization should consider the human element and revise their cyber-security policy to contain three essential components.

1. *Understand the risk and avoid the problem.* Just because a system has never been hacked is no justification to feel completely secure. Yet, there seems to be a tendency to stay with what appears to be working only because no data has either been breached or identified as being breached. This is no time to be complacent. The risks are there, and managers have to accept that fact-of-life and work with technology to assure data protection on a regular basis.

2. *Challenge what you are being told*. The foundation of this component is learning from the experience of hacking victims. Executives and administrators need to mandate data breach studies for comparative analysis. There is no better way for the organization to determine if its data is equally vulnerable and susceptible to similar attacks. Review the human element along with the history. "We've got it covered" may be only a temporary truth.

3. *Test the people with the process.* Require a full examination of infrastructure technology, data monitoring committee (DMC) policies, alert policies and ability to protect the system. Testing should be conducted on a frequent basis and should not be limited to technology. Investigate the human element along with the infrastructure to pinpoint the relevant metrics that can yield actionable protective measures. Independent technology consultant Dave Malmstedt put it best, "Keep trying to break what you have to make sure no one else is going to break it."

Conclusion

Technology cannot be taken for granted no matter how revolutionary the newest so-called game changer appears to be. Yes, the latest encryption models may stand up well against hacking and data breaches, but those should in no way be considered flawless especially if they are limited to one level of encryption. No database, regardless of its sophistication, is immune from a successful attack. The fact is: innovative technology by itself cannot be counted on to ward off incursions from motivated and talented cyber-criminals.

That's why it is important to return to the human element of cyber-protection. Cyber security works best when the three policy components *1) Understand the risk and avoid the problem, 2) Challenge what you are being told* and *3) Test the people with the process* are constantly and regularly reviewed by those responsible for implementing and managing them *every day.* The processes will only be as good as the people who sustain them.

Company Credentials

Global Data Sciences, Inc., Aurora, Ill., provides scientific, data-focused approaches to developing and executing sound strategies to increase company value in the global environment. We specialize in identifying hidden opportunities in enterprises through proven techniques that produce tangible and measurable results. Among our many areas of expertise are global operations, process and procedure optimization, systems integration and optimization, and cyber-security and data forensics. Tel: (630) 299-5196. Visit our website at www.globaldatasciences.com. Email us at info@globaldatasciences.com.

References

[1] "Cyber Attacks on U.S Companies since November 2014." Riley Walters. *Issue Brief #4487 on Cyber Security."* The Heritage Foundation. November 18, 2015.

[2] "The New Security Paradigm." Joe McGrath, UNISYS. WCIT presentation. 2006.

[3] "Top 10 Most Devastating Cyber Hacks of 2015." Ben Rossi. *Information Age.* December 2015.

[4] "*2015 Cost of Cyber Crime Study: United States*." Ponemon Institute. Sponsored by Hewlett Packard Enterprise. October, 2015.

[5] Walters 2015.

[6] Rossi 2015.

[7] "SEC Charges Investment Advisor with Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to Breach." U.S. Securities and Exchange Commission. September 22, 2015.