Andy Was Right
Information Security 2010 – 2020

By Frederick Scholl – ISSA member, Middle Tennessee, USA Chapter

This article reviews three high-level IT trends that could lead to increased information security hazards over the next decade. A suggested approach for managing security risks in this environment is given.

Abstract

This article reviews three high-level IT trends – the growth of data, globalization, and the consumerization of IT – that could lead to increased information security hazards over the next decade. A suggested approach for managing security risks in this environment is given.

In 1996 Intel's Andrew Grove published his guidelines for business strategy success, *Only The Paranoid Survive*.[1] I believe this title aptly describes data security now through 2020. Things are going to get worse before they get better. This is a result of the rapid changes in the systems that need to be protected, not from the lack of security technology or frameworks. To understand data security requirements through 2020, we need to analyze the broad changes to IT and to the systems and information we need to protect.

In his book, Grove describes the concept of a "strategic inflection point," a change in the way business is done. A strategic inflection point can result from two or more industry trends combining sympathetically at the same time. It is both a threat as well as opportunity for those who are able to adapt quickly. In this article, I describe three trends in the IT industry that will affect how information is secured effectively over the next 10 years. These trends are combining to create a strategic inflection point and a need for new ways to secure information.

The growth of data

It's pretty familiar to everyone that we are drowning in data. Who has time to read even a small fraction of the email (or snail mail) received every day? Yet it is the job of information security to protect *all* of this data. Recent estimates[2] put the worldwide annual generation of data at 1250 Exabytes (1 EB = 1 Billion Gigabytes), growing at a 60% annual growth rate. In 2020 we can expect the annualized data generated to be 125 Zettabytes (1 ZB = 1000 EB). More security professionals will need to be focused on protecting this sea of data, rather than just protecting hosts and networks.

Information security approaches from the past 10 years will need to adapt to keep up. With a 60% compound annual growth rate, today's security manager will be asked to secure 100 times more data in 2020. This data will be stored in more locations and shared with more partners than ever before. Business operations in more firms will be increasingly reliant on continuous availability of data. More data will need to be disposed of effectively at its end of life. Rather than investing only in perimeter security or even distributed security to protect this information, firms will need to implement strong data governance[3] programs. The information security role should play a lead in this effort. The core definition of data governance includes security and privacy, data quality, and data life cycle. If the data is wrong, it does not really matter if it was maliciously changed or not; the business operation is adversely affected. The well-publicized mortgage documentation mess – expected to cost upwards of $10B to resolve – is a perfect example of the lack of good data governance.

Globalization

Globalization is presenting major threats to information security. While the terrorist threat is better publicized, other types of information security threats may be more damaging in the long run. Globalization, combined with increasing

1 Andrew Grove, *Only The Paranoid Survive*, Bantam Doubleday, 1996.

2 "Data, data, everywhere," interview with Kenneth Cukier, *The Economist*, February 25, 2010 – http://www.economist.com/node/15557443 (accessed 11/26/2010).

3 The InfoGov Community – www.infogovcommunity.com.

Internet access around the world, means for security that we have less and less confidence as to whom and what is entering our living rooms and conference rooms.

Increasingly, we do not know where the hardware and software in our systems come from. I was reminded of this problem recently after purchasing a new brand-name office wireless router. When the router did not work properly, I contacted the vendor technical support. I was surprised to learn that my router's three year warranty had expired two months previously! Obviously the router had been remanufactured by an unknown party, put in a new box, and possibly now contained unknown firmware as well.

If the hosts and software being protected by information security are themselves of unknown integrity, providing information assurance for the data becomes orders of magnitude more difficult. Problems will range from hostile code compromising data confidentiality or integrity to availability problems caused by faulty technology such as that in my office router. Over the next 10 years we will need to figure out how to assure the integrity of our systems in a free marketplace economy. A recent *Wall Street Journal* headline – "Security Fears Kill Chinese Bid in U.S."[4] – highlighted the problem. According to the article, Sprint Nextel rejected Chinese telecommunications equipment because of security concerns from some U.S. lawmakers. U.S. Senate Bill 3480 (Lieberman/Collins) is an example of government efforts to improve supply chain security through legislation and regulation. This bill and others like H.R.6423 will be debated in coming months. It's pretty clear to me that industry will not protect its customers in this area and that some type of government assurances (regulation) will be necessary.

Globalization appeared again recently when a neighbor called urgently one evening to let me know that a family member's business had been hacked and that $350,000 had been transferred to an Eastern European bank. Fortunately the business owner had contacted an attorney who had, in turn, contacted the FBI. Through three days of hard work, they were able to get this transaction reversed when the European bank opened on Monday morning.

It is easy to think that this type of thing is happening only to the other guy or other company. But, as Stewart Baker[5] has estimated, only 10% of the world has more than $65,000 in net assets. In 2010 that still leaves 6.3 billion people with fewer assets. This number is growing as is the Internet connectivity within the group. For the bad actors in that group, people and businesses in developed countries become "targets of choice." Global bad actors are also skilled at playing support roles when home-grown criminals take the lead.[6]

4 J. Lublin and S. Raice, "Security Fears Kill Chinese Bid in U.S.," *The Wall Street Journal* (November 5, 2010) – http://online.wsj.com/article/SB10001424052748704353504575596611547810220.html (accessed 11/26/2010).

5 Stewart Baker, *Skating on Stilts*, Hoover Institution Press, 2010.

6 M. Wilson and W. Rashbaumm, "Real Patients, Real Doctors, Fake Everything Else," *New York Times*, October 13, 2010 – http://www.nytimes.com/2010/10/14/nyregion/14fraud.html (accessed 11/26/2010).

A continuous threat environment can be met only through a continuous improvement of security processes.

International cybercrime is not growing from scratch. It is not a start-up enterprise. It is building on a thriving global shadow economy that comprises failed states, transition states, and consumers mainly in wealthy countries. International cybercrime networks have roots in the many networks supporting illegal trade in everything from caviar to heroin to tobacco products to automobiles. These illegal networks were analyzed and given the name McMafia[7] by author Misha Glenny, because of their global reach and global ambitions. As international criminal gangs become increasingly network savvy, they can make use of their existing business know how and contacts to carry out more sophisticated cybercrimes.

Consumerization of IT

As IT becomes increasingly consumerized, security challenges multiply. Leading edge IT products and services are increasingly aimed at mass markets and are no longer the purpose-built enterprise, government, or military applications. At one time, enterprises relied on such purpose-built applications. In the best-practice case, security could be assured with controls built in to the SDLC process itself. Now business users can select SaaS applications that may or may not meet the corporate security policies and standards. The growth of self-service applications on the Web is short-circuiting the traditional IT department and changing the role of the information security function.

A dramatic example is the growth of consumer-oriented mobile computing platforms. Ray Kurzweil predicted in 1999 that in 2019, "You [will] do virtually anything with anyone regardless of physical proximity."[8] If anything his prediction will be fulfilled in less than nine years. At one time, users followed a corporate standard for mobile platforms along with all other platforms. Now increasing consumer-oriented choices of mobile technology are making this more difficult to enforce. The product cycle times in the consumer space are simply too fast for many enterprise IT and security departments to react.

Another aspect of consumerization is the so called "Walmarting of IT" in which cost considerations take precedence over everything else.[9] This is especially true for "legacy systems" that keep the business running. It is understandable that business wants to reduce annual costs for IT applications. But will system security take a back seat in this process? Will security controls be updated for legacy systems as the threat environment changes?

7 Misha Glenny, *McMafia*, Vintage Books, 2008.

8 Ray Kurzweil, *The Age of Spiritual Machines*, Penguin, 1999.

9 "Is Walmarting IT a good idea?" – www.ciotalkradio.com, October 6, 2009.

Solutions

How to secure information with these forces of change at work? Any proposal must take into account today's mandate to do more with less. In addition, most security programs do not fall within executive management's top ten initiatives. The effective security program must also operate within this constraint.

Technology is an often proposed solution. This, by itself, will not provide the answer. As Donn Parker succinctly put it nearly ten years ago: "It is futile to rely on technological protection."[10] True then; true today; true tomorrow.

The perfect storm may be business users on consumer-grade mobile platforms accessing confidential data hosted in offshore cloud computing facilities.

Another common security approach is to rely on compliance to audit control checklists. While necessary, this approach will not be sufficient to secure our organizations in a rapidly changing threat environment.

I believe we can best meet the new threats by implementing security as a business process. The two key words to analyze here are "business" and "process." The next issue is how to get there if your security program is not already managing effective security business processes.

Since threats now are coming from global "businesses" and not lone technologists, information security needs to respond in kind. A business approach will be necessary to respond to the new threats we will see over the next 10 years. A business solution is a holistic solution that makes use of all enterprise resources available including technology, process, people, and partners. It means effective collaboration between information security, IT, HR, legal, purchasing, and operational business units. Of course, this is not a new idea; what we need now is more success at implementing it.

Second, we need to focus on security processes; this is the only approach that can offer both cost savings as well as continuous improvement in risk mitigation. Each business needs to construct its own process framework and implement active management of those processes. The common element is the continuous improvement approach: the key to effectively managing security. In the past, we could deal with a virus outbreak one year, a new worm the next. Now we have a continuous threat environment which can be met only through a continuous improvement of security processes.

Security frameworks such as ISO 27001 and COBIT focus at a high level on continuous process improvement, using the Plan-Do-Check-Act (PDCA) approach. But often these frameworks are implemented as a series of controls to be audited on a regular basis. Supporting these controls will be processes such as access control, change management, secure systems development, risk management, monitoring, communications, etc. The long-term key to successfully implementing any of these frameworks is to focus on the end-to-end security processes, as well as the auditable controls.

How to implement an effective process-oriented security program built around continuous improvement PDCA principles? This may seem to be a serious challenge and require that the enterprise go up a staircase from maturity level 1 to level 5. Many enterprises are operating at levels 2-3 and having difficulty going beyond that. A head-on approach to making improvements can be very difficult given the usual priorities of users and business leaders.

Instead we can use the principles of *Kaizen*, or continuous improvement, to gradually transform the security program. Each security event or incident should be seen as part of a larger end-to-end process and an incremental step taken to improve that process. New security initiatives can be implemented as part of major IT and business programs and then rolled out as best practice. Gradually, over time, a full-fledged, continuously improving security program will be in place. Visually, this is like the game of Go where opponents battle to take over the board area, expanding from multiple points on the board. Progress toward victory is made by expanding out from multiple starting points. It is instructive that the *Kaizen* quality approach (then known as TWI, Training Within Industries) was first introduced to U.S. manufacturing plants during WW II as a way to deal with labor shortages and vastly increased manufacturing requirements ("do more with less").[11] Today we have new global security threats but the same mandate to manage those threats with fewer available resources.

Conclusion

Trends in information and information systems will make the job of securing information increasingly difficult over the next 10 years. The perfect storm may be business users on consumer-grade mobile platforms accessing confidential data hosted in offshore cloud computing facilities. To meet these threats enterprises should increasingly adopt a business process response. The business approach utilizes all of an enterprises's resources, as needed, and not just IT resources. The process approach enables a continuous improvement of security and will make it possible for managers to meet the continuously worsening threat environment with the same or fewer resources.

About the Author

Fred Scholl, PhD, CISSP, CISM, CHP, is a security consultant based in Nashville, Tennessee. A member of ISSA Middle Tennessee Chapter, he may be reached at freds@monarch-info.com.

10 D. Parker, "Lessons from 30 Years in Information Security," *The ISSA Journal*, January/February, 2001 – issa.org//Library/Journals/Older/2001/Parker%20-%20Lessons%20from%2030%20Years%20of%20Information%20Security.pdf.

11 Robert Maurer, *One Small Step Can Change Your Life (The Kaizen Way)*, Workman Publishing, 2004.