1
The World of Cyber Security in 2019

"The semantic Web – what is called Web 3.0[1] – is commonplace in 2019. The start of the Internet and the World Wide Web is the stuff of legacy and lore. Amid the concerns of ICT security is another dimension – the clash of virtual realities such as between the Second Life® virtual world and the physical lives. Decisions in the virtual world drive material reactions in the real world – as they are now one world with no safeguards in place."

Executive Summary

It is 2019 AD or 28 AW (after the Web), counting in years after the introduction of the World Wide Web.[2] Contrary to some predictions, ICT systems continue to be one of the primary agents of change in our lifetimes and in the history of humankind. The pace of change has been nothing short of spectacular. There have been many winners and losers as the exponential growth of technology gives rise to new and wider social divisions. This change ripples through societies, cultures and nations with unintended consequences that are too numerous to count.

[1] www.wikipedia.org - Web. 3.0 is one of the terms used to describe the evolutionary stage of the Web that follows Web 2.0.

[2] www.wikipedia.org - World Wide Web is a system of interlinked hypertext documents accessed via the Internet.

In hindsight, one can see where things went right and where they have gone terribly wrong. Protecting ICT systems has been one of the great challenges. With 12 years of history, Web 2.0 continues to serve, transform and interconnect the world's cultures. Nothing is left untouched by the Web 2.0 generation as worlds that were once physically and logically separate are now inextricably linked. Generation Y and Generation Z (also known as Millenials), born in the age of computers and the Internet, run the physical and virtual worlds. It is a new world, but is it "brave" or is it "foolhardy."

The threats to cyber security in 2019 are many. How did things get to this point? In hindsight, the answer is all too clear. It just happened degree by degree, like the slow-rising temperature in the cauldron. The gradual slide was something that happened even as it is clear that we could have and should have integrated security into our ICT systems. It is not that the technical know-how was missing, nor was it something that came as a surprise. It was a ripening awareness of the vulnerabilities. By the year 2009, it was understood that security had to be an integral part of system design yet by the absence of forethought, understanding and leadership, the vulnerabilities in ICT systems were left unaddressed. It is 2019 and it's time to pay the piper.

It was a sword that cut both ways; the standardization on all-IP systems is what allowed the world of data, voice and video to blend in ways that created the value of next-generation systems. Web 2.0 applications would not have achieved its broad appeal without the convergence of IP systems. It also meant that the vulnerabilities were many and were both *transmuted*[3] across the different media and infrastructure domains and replicated across the many nodes in the complexity of the Web 2.0 world. Encryption can be broken with powerful computers. Quantum computing is in our midst; even strongly encrypted national systems are at risk.

[3] Transmutation, is used to describe the phenomenon where as an example, a virus delivered by email to compromise computers is now re-crafted for telephony.

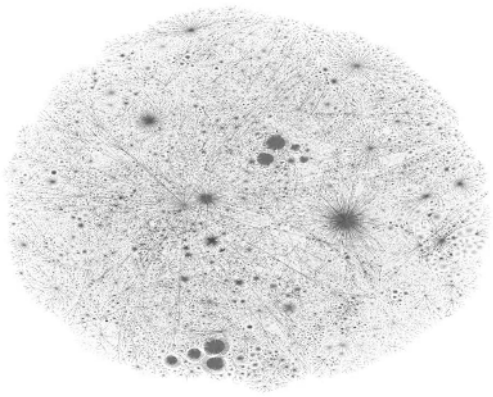

Figure 1.1 Internet Mapping

It is a situation that could have been avoided; the challenge now is to find a way to fix an installed and complex array of systems that are used for almost every type of business. Unfortunately, the complexity of system management and data stored in a dizzying range of formats cannot be remedied without starting over. Bill Cheswick's Internet mapping from 2009 shows a picture of this technology galaxy as ganglions interconnected like a constellation of stars (Figure 1.1). Today, with its accelerated growth, it looks more like a round brown blob – the number of nodes so large that one cannot see space between their connecting points.

Security in complex systems implemented after they are in production is at best a patchwork fix. However, patchwork security is ill-suited to counter the means, motive and opportunity; the deadly triad law enforcement recognizes as the source for crime. The opportunities are endless with global online access. Gone are the constraints of physical separation. The notion of nation-states means little in the global Internet; even parallel private versions of the Internet can be breached.

Vulnerabilities are so commonplace that in the period from January 1, 2007 to December 31, 2007, the IC3 (Internet Crime Complaint Center) Website received 206,884 complaint submissions.[4]

---

[4] Federal Bureau of Investigation, Bureau of Justice Assistance, The National White Collar Crime Center – "*International Crime Complaint Center 2007 Internet Crime Report*" (Washington, DC 2008), 1.

People continue to be the weakest link in the chain, the underlying fact in the social engineering schemes. Crime follows money, and with e-commerce and businesses dependent on online transactions, there is plenty of money-motivation.[5] Politics and world tensions are also motivating factors. Demonstrations have now moved online. Citizen unrest that used to make itself heard in the streets is now expressed through distributed denial of service (DDoS) attacks.[6] It is a very difficult state of affairs. The remedies available are appearing as items on a menu of poor choices dependent upon detecting and responding to a "zero-second" threat. It takes practically no time to form and launch an attack. The average password can be broken in less than ten minutes; the break-in, undetected, is only a prelude to the actual attack.[7] How does one detect and respond to "zero-second" attacks?

Thankfully, it is not the year 2019 as of this writing. 2019 is still some years in the future, and Web 2.0 is still taking shape, as are the next-generation networks that will be the underpinnings of the latest applications and services. What steps can be taken now that will yield a more positive outcome; one where security is a central part of the system design and applied in a balanced approach to the risk? How much time is there? Is there a tipping point when it becomes too late? How close is that point? Interesting questions, indeed and they need immediate answers.

A recent article in CSO Magazine *stated that, "the most risky mobile device is the laptop computer and the number one concern is the inability to properly identify and authenticate remote users."*[8]

The concern is with what can be done *now* using the methods and the technologies already available to set in place the idea that security can be *designed in* to the complex networks that are getting installed now and that will exist in 2019. Web 2.0 is still evolving and it remains

---

[5] "*International Crime Complaint Center 2007 Internet Crime Report*". In 2007 monetary losses totalling $239.09 million with a median dollar loss of $680.00 per complaint

[6] Jeremy Kirk, *Computerworld*, "Estonia recovers from massive DDoS attack", May 17, 2007.

[7] www.hackosis.com.

[8] Dr. Larry Poneman, *CSO Magazine*, "Cyber Crime: The 2009 Mega Threat", www .csoonline.com/article/print/470968 (December 16, 2008).

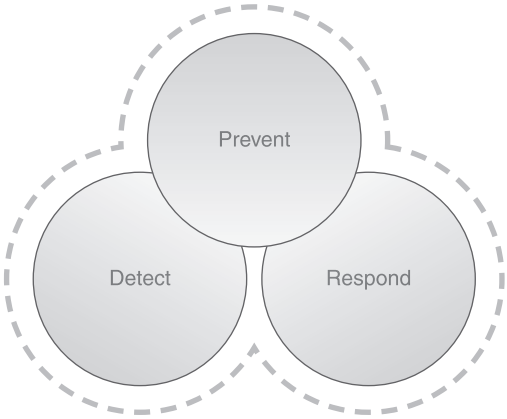

Figure 1.2 The Security Triad

the next great technology promise. There is still a chance to correct the path and *design in* a more secure destiny.

Consider another triad – the security triad of *prevent-detect-respond* as the context for all security functions (Figure 1.2). The *prevent* part of security is where the technologies around *designing in* security fit in and is the focus of this book. Prevention includes another word, overused perhaps, but still significant to this discussion. The word is *trust*. Every day people make decisions about whom they should trust. It remains to be seen whether the makers of the ICT companies will design in the security to achieve trustworthiness as a measurable attribute.

On the question of time, the point of no return after which it will be nearly impossible to achieve a positive outcome for Web 2.0 security is rapidly approaching. IPTV is already gaining a foothold and Voice over IP (VoIP) is already strongly embedded in the corporate world. Video in all its manifestations is being transmitted over IP networks. Separate infrastructures for voice, video and data are collapsing into one flat IP world.

There is also the question of risk. The paradox of Web 2.0 is that many millions of individuals are willing to incur a potential loss of privacy by opting into social networking sites in spite of the apparent risk of identity theft and other abuses that come from sharing personal information on these Web sites. Those who engage in social networking clearly believe that the benefits outweigh the potential risks

Although this book is indirectly concerned with the question of responsibility, it is directly concerned with the questions of *what* can

be done and *how* to protect the new Web 2.0 environment, a set of issues that are addressed in Chapter 2. Before embarking on a path that will lead to better security, one must first discover how to measure security and then implement the systems that accomplish this measurement. This process should be based on actual measurements; and be more science than art. "There cannot be a greater mistake than that of looking superciliously upon practical applications of science. The life and soul of science is its practical application."[9] Trust can be measured, given a score, and improvements made on that score while making more informed judgments about levels of access on the basis of this score in real time. This is the value of prevention in the security triad and the point of focus.

Product developers and security professionals possess the know-how to achieve more secure environments. This book presents a set of fairly straightforward rules, and introduces a framework for security design developed in 2003 by scientists at Bell Laboratories.[10] These scientists began by asking themselves some very basic questions about how to measure, baseline and integrate security into complex ICT networks. Finding the answers unsatisfactory, the scientists decided to develop a framework to solve this problem. The framework measures security, identifies the gaps and implements remedies with consistency, rigor and practicality, focusing on such issues as "just enough" security. It is time to get started – time is of the essence.

General Review of Security Challenges

There are new security challenges each time someone invents a way to automate or integrate human activities with ICT systems. In the world of finance, this point was made clear with the scale and speed of the losses that occurred at Société Générale in 2008.[11] In ICT systems, unlike the physical world of vaults and walls, the impact can occur so much faster and reverberate with much greater damage.

---

[9] Lord Kelvin - PLA, vol. 1, "Electrical Units of Measurement", May 3, 1883.

[10] Ashok K. Gupta, Uma Chandrashekhar, Suhasini V. Sabnis, Frank A. Bastry, "Building secure products and solutions," *Bell Labs Technical Journal*,Volume 12 Issue 3, Pages: 21–38.

[11] Nicola Clark and David Jolly, "French Bank Says Rogue Trader Lost $7 Billion," *New York Times*, January 25, 2008.

Web 2.0 poses the latest of these challenges. The repercussions of loss in the cyber world are nonetheless physical; people can lose their jobs, and the public is harmed. Consider these challenges as they evolve in the services and applications of Web 2.0.

Content is king

Much attention has been paid recently to content protection. Most of this concern around content is directed at *end-user applications,* such as spreadsheets or word processing files. Content-filtering products have been primarily about "gate-checking" to make sure protected content does not leak outside the network. Still, content is found in all layers of the network and not just in a format that is recognizable to end-users. In the network infrastructure, content can take the form of account information such as billing. In services applications, it can include profile information used in target marketing. In other applications the content is the data stored in the databases and presented in application servers. Yet, no matter in what form it appears it is all content and it can all be lost, tampered with and subverted to harm people and damage systems.

Consider further the meta-data[12] content in the infrastructure and services as one example.

Target marketing makes use of business intelligence to match the right marketing information with the right target population or even the right individual. Its criminal equivalent is "spear phishing" that applies "business intelligence" gathered about wealthy people but for malicious purposes. It is still, relatively speaking, a low-level problem. What if more aggressive criminal organizations or governments were to apply these very same "business intelligence" techniques, using the meta-data content to target populations, with the purpose of keeping power, gaining power or stifling dissent? Content protection is more than just keeping business files from leaking outside the network perimeter. Consider also the background information (the meta-data) about the data, which can be as simple as the demographics of Web surfing being used for constructive or criminal purposes. Content even in the form of meta-data is king and it needs to be protected.

---

[12] Meta-data examples: "data about other data" - MP3, cookies, visited web sites, etc.

Network criminals target another form of content, the network architecture to determine detailed information about the operating systems, patching levels, and location of critical assets. By burrowing deeper into the network, the attacker can determine the access controls, break those controls and initiate the final phase of the attack. The final stage of the attack can take place in a few seconds. It may involve efforts to steal, modify, or even to encrypt the content or disrupt the service. Using database encryption as a denial of service technique an intruder can keep a business from accessing its database and disrupt its operations. This can be devastating to a business in the real-time and global online environment where even seconds of downtime can translate into millions of dollars in lost revenue.

Broadband wireless security

Fourth-generation (4G)[13] broadband wireless communications and all it promises for creating ubiquitous communications is under development. The taste of this promise is already present in 3G[14] systems. For anyone carrying a 3G wireless card, there is much to complain about, but just try to take their 3G card away and one will find that "stickiness" has already developed. The wait for 4G is filled with great anticipation. One can envision a great range of business activities that will blossom from this freedom to connect anywhere with high-capacity bandwidth that will truly enable open (non-wall gardened)[15] Web services. Has the security required for 4G systems been considered?

There is, in fact, much to consider. 4G in all its versions seems poised for success, and will undoubtedly create a demand that is only

[13] www.wikipedia.org - 4G is an abbreviation for Fourth-Generation, is a term used to describe the next complete evolution in wireless communications. A 4G system will be able to provide a comprehensive IP solution where voice, data and streamed multimedia can be given to users on an "Anytime, Anywhere" basis, and at higher data rates than previous generations.

[14] www.wikipedia.org - 3G is the third generation of telecommunications standards and technology for mobile networking, superseding 2.5G. It is based on the International Telecommunication Union (ITU) family of standards under the IMT-2000.

[15] Non-wall Gardened - where the network operator can act as a channel. With this model, smaller service providers, enterprises and developers can now use more advanced mobile services in a simple way to provide specific end-user services.

in the beginning stages. 4G will have to be highly available, reliable and secure to meet expected demand.

With expanded accessibility and capacity will come expanded use of personal, business and government applications, and these will gain critical mass that is far reaching. From a security perspective, tens of millions of 4G subscribers added to hundreds of millions of sensors (machine-to-machine accounts) require systems that must scale in size, in features and that must be assured. Simply put, there is an inherent degree of fragility in a highly shared, highly limited RF channel that is used for wireless communications. This fragility is not there in the same measure for wire line systems that can have high bandwidth dedicated to the subscriber at the aggregation point.

Cyber Security as the Friction and Latency of Business and Government

The value of ICT is to enable businesses to compete on the basis of agility and scale, allowing the business to adapt to market conditions faster and with greater efficiency to bring the right products or services to market at the right time. Agility is, in large measure, about a reduction in process latency and friction. Although the world is highly interconnected, the reality is that interconnectivity is still in its early stages.

As rapidly as these new capabilities that interconnect technology are entering mainstream, cybercrime is growing at an even more alarming rate.

Governments are not immune as the public demands e-government accessibility and efficiency. Yet there are numerous examples of government systems that have been compromised when sensitive data has been lost, and the trust between government and its people breached.

Web 2.0 is the next step in the maturation of the Internet, but is there sufficient understanding of the risks and the impact that can occur when systems operate without the necessary protections?

Will security incidents ultimately choke off the success to the point where outages make customers reluctant to move to more advanced online services? If not the incidents themselves, the burden of over-compliance is another form of friction; security not in the service of the business but acting as nothing more than sand in the machinery. There

is a need for prudent regulatory requirements: the number of existing regulations will remain – they are not going away. Additional regulatory requirements can be anticipated in response to the public's increasing concerns that companies are not safeguarding information as they should. Many argue that cumbersome regulations, such as California's SB 1386, are already in place as regulators respond with legislative instruments and penalties for accountability.[16] Passed in 2003, SB 1386 was the first legislation that was enacted to protect against security breaches. Since then most other states in the United States have passed similar laws.

There are unintended consequences that result from passing this type of legislation, such as diminished business agility. United States businesses subject to the Sarbanes-Oxley regulation are already smarting from the high overhead costs such regulation engenders. It isn't just public companies, but virtually any company that conducts business in the United States is impacted. Many blame over-regulation on the tectonic shift of securities exchange listings from the U.S. to the exchanges of London, Singapore and other major global financial centers.

Impact also comes in the form of losses created by security incidents. This is latency and friction in its worst form. Efforts to quantify losses reveal how difficult a task it is to get companies to collect and report this information. The CSI annual cybercrime survey[17] repeatedly discusses the dilemma of too few companies willing to report cybercrime information. This is also friction – the grit that breaks down the ability to clearly express the problem to policy leaders.

Protecting Web 2.0 Data

The information flow in the Web 2.0 model has specific risks beyond the general risks with IP-based systems and the Internet discussed up to this point. These risks go hand in hand with what makes Web 2.0 a more challenging environment to protect. It's a virtual place where conventional boundaries don't always apply and where the spirit of open exchange may conflict with privacy

[16] http://info.sen.ca.gov/pub/01-02/bill/sen/sb_13511400/sb_1386_bill_20020926_-chaptered.html.

[17] http://www.gocsi.com/

concerns. Chapter 3 examines in some detail what makes Web 2.0 security particularly challenging. Three issues are of particular concern: control of the data, control of identity and privacy, and the value of virtual assets.

The discussion first considers content stored on public sites. These may also include software as a service (SaaS) sites that, together with consumer-driven sites, may have an implied, if not explicit, expectation for using the stores of data for target marketing. A variety of questions, issues and challenges stem from this condition of open exchange and they begin with the question of control. Data that is used in a Web 2.0 application provides a great advantage to the online service provider when it is data provided without strings attached. In some cases this data is the business. Take away this control and the business model of target marketing starts to unravel.

Who owns the data and how should control be handled? In the first point of view, it is the organization providing the service, whether it is the Web 2.0 company, a hospital, a government agency or a financial company that controls the data. The opposing view, more closely represented in European countries, is that companies storing the data can only use it in a very narrow and strictly controlled role. The end-user controls the information, and the end-user must expressly authorize any further use of the data.

Despite privacy statements provided by U.S. companies to their customers, the present balance of control tilts almost exclusively to the advantage of the company. In this instance, the end-users have given up their rights to control. Many systems are in fact designed with few, if any, opt-in end-user controls. It becomes clear after reading the fine print but few people take the time to do so.

If information is power, then there is a power base growing in the Web 2.0 + world and in every large organization that is collecting data either directly or indirectly as in the meta-data discussed earlier. The end-users have given up control. Where is the balance? Is a medical file containing an x-ray taken at a hospital safe from abuse by employees, insurance firms, hospitals and pharmaceutical companies? Should we trust that the company will protect this medical information adequately?

In the law enforcement triad, the *means* exists in the tools of the criminal world, the *motives* are many and the *opportunities* abound. The opportunities are found with the inherent vulnerabilities that exist in complex systems and the absence of a legitimate basis for trust. Until

the many dimensions of the cyber security problems can be measured the problem cannot be corrected.

Information governance in an enterprise is hard enough. In the Web 2.0+ world, who safeguards the interests of the end-user when the business model is explicitly designed to support the application of information for target marketing or other similar purposes? This question is difficult to answer, because no one has clear governance over the information produced. Trust in the cyber world must be measured or it is nothing more than marketing and should not be considered a proxy for making governance decisions about finance, health or privacy.

Protecting information in the Web 2.0+ world, where it is about protecting the value of virtual presence is paramount for personal and financial risk management. A Web 2.0 company's value is not in its physical plant, but in its Web presence and infrastructure. Insuring physical assets is relatively simple. Insuring a cyber presence is radically different because it is usually more difficult to quantify. The value of an online company is almost wholly dependent upon brand value, the services offered, how well the information and its technology systems function and how well they are protected. The physical assets have, by comparison, negligible value.

When an e-commerce company has a market capitalization in the tens of billions of dollars, understanding how to protect this virtual world is exceedingly important. In the real world property is valued in terms of physical assets. In the Second Life world virtual property is sold with real money.[18] How is the physical asset to be insured? It is all about protecting Web presence, an ephemeral notion that does not fit the model of insuring physical assets and where cyber-value and cyber security is paramount.

The Present Models for Cyber Security are Broken

The current practice of cyber security is lacking in many regards, but it is not possible to address the problems until the root causes are understood. The identification of root causes starts with ICT systems

[18] http://secondlife.com/whatis/land.php - The Second Life® 3-D virtual world is created by its Residents. Since opening to the public in 2003, it has grown explosively and today is inhabited by millions of Residents from around the globe.

sold to a market that places the responsibility for security on the end-user. This condition is consistent no matter whether the end-user is a consumer or a company providing services that because of the size of the market makes up a part of the national infrastructure. At an individual level, consumer-owned personal computers could hardly be considered part of the national infrastructure. Taken in large numbers they are the end-tools used for all forms of online transactions and in a national emergency may even serve as the primary means to conduct government business (in a health crisis situation government employees will be expected to work from home connected to the government data centers). It is not just home PCs that have to get patched, it is also the hundreds of thousands of computers and servers in government agencies and in utility services.

Web browsers are used to perform a wide range of functions such as online transactions. At the same time that they have gained many new features Web browsers have also become more vulnerable and can be compromised by malware that steals identity and account information. The practice of cyber security must first be repaired before a wholesale move into the Web 2.0 + world can be considered, much less undertaken.

Recall the security triad. *Prevention* has been all but ignored and replaced by an almost exclusive reliance on detection and response security technologies incapable of compensating for all the inherent vulnerabilities in complex systems. The cost of security is too high, not enough results are being delivered for this investment and as the dependency on these same technology systems grows, so do the risks.

This trend is not exclusive to the business world. U.S. government agencies are rated with the Federal Information Security Management Act (FISMA) scorecard on how well they are meeting security regulations with many of them getting "green" scorecard ratings. The truth is they are a poor reflection of how well the systems and the data are secured. A simple question such as how many laptop computers are there in the inventory will stump many an agency that scores "green." If this question cannot be answered with certainty at all times, how is an agency to know what data is put on these laptops and whether the data is being protected?

"The stolen laptop at Veterans Affairs (VA) was a failure to manage what employees do," says Boots. "VA had a good FISMA score card, the system including the stolen laptop had been certified and accredited.

From a FISMA standpoint, all was well." In other words, compliance doesn't always prevent breaches.[19]

The same situation exists in Europe, where reports are appearing in the press on a regular basis that detail sensitive data losses. This begs the question: do governments have the competency to protect the data its citizens have entrusted to them? Citizens are questioning whether government agencies can be trusted to protect identity information as in national identity cards or electronic voting information. There is reason to be concerned. Global spending on computer security topped US$7.5 billion in 2006.[20] Is it yielding the security that is needed?

A systemic problem

The problem does not begin with government agencies or with businesses. Consider the fundamental problems and whether the technology vendors are applying the right security controls to the systems that are sold to businesses and government agencies. What about the companies that deliver network services. Are they applying security in the right measure? A bit closer to home, are the businesses purchasing technology solutions making security a key requirement for purchase?

The answers to these questions are a mix; there are clearly positive efforts, though on the whole there is much that needs improvement. The answers discussed in the following chapters suggest that the models of cyber security are in need of repair. They also suggest that the systemic remedies start with the right models – models that can be used to guide the path of correcting significant security issues and to produce secure and reliable technology systems. Preventing security issues from happening can start yielding better results.

As the Web 2.0+ world begins to take firm hold in the business world, it is time to apply a better model based on the principles of science where measurements are paramount. To solve this problem in the long term, the integrity of systems and data must be measured and assured and this is even more urgent in a world of interconnected systems, complex supply chains and business partnerships.

[19] Kellie Lunney, "Cyber Security chiefs keep a low profile", *Government Executive Magazine,* September 27, 2007, http://www.govexec.com/story_page.cfm?articleid=38145.

[20] Gartner, 2007.