Bruce McConnell
Global Vice President
EastWest Institute
bwm@eastwest.ngo
Paris, September 29, 2016

The Cybersecurity Threat Landscape

Merci bien, Sebastien, et merci a Denis et SCOR, pour l'opportunite d'ouvrir ce conversation ce matin sur le sujet Cyber Risk on the Rise. It is always a pleasure to be in Paris. And what a great introduction to the topic from Denis. I have a feeling this morning is going to be somewhat gloomy, focusing on the problem.

[Maturity of conversations.] I am looking forward to tomorrow when we will talk about solutions.

I am Bruce McConnell, Global Vice President of the EastWest Institute or E.W.I. EWI is an independent non-governmental organization that works to reduce international conflict, addressing seemingly intractable problems that threaten world security and stability. EWI is 36 years old, with headquarters in New York and offices in Moscow, Brussels, Washington, and where I work from – San Francisco.

EWI works closely with governments and companies around the world to promote security. We work both bilaterally and globally. For example, we sponsor a party-to-party dialogue between the Chinese Communist Party and the US Democratic and Republican parties on security issues such as the South China Sea. With Russia we host a lower-level dialogue aimed at reducing the flow of narcotics from Afghanistan. My portfolio at EWI focuses on issues that involve multiple players. Cyberspace security falls under that umbrella.

EWI focuses on conflict reduction around security issues. We work to reduce the likelihood that the inevitable disagreements among powerful actors on the world stage will lead to major disruptions in the global economy or in the fabric of international security. Cyberspace is a domain where we believe there is a high likelihood of miscalculation, of unintended consequences that could lead to such major disruptions.

This morning I want to start by looking at cybersecurity risk in a geopolitical context. I will then drill down into the enterprise risk picture, and finish with some observations about risks to the insurance industry.

So, cybersecurity and the geopolitical threat picture.

Three years ago US national security advisor Susan Rice observed that the world's "most vexing security challenges are transnational security threats that transcend borders: climate change, piracy, infectious disease, transnational crime, cyber theft, and the modern-day slavery of human trafficking." Today, one could add migration, violent extremism, and the safety of fissile nuclear materials to that list.

These issues share at least two characteristics: first they are accentuated in their severity by modern technology. The bad guys, both state and non-state actors, are well equipped with the latest computers, communications equipment, and weaponry, and their ability to use these tools is enhanced by their access to global networks.

Second, for these issues that transcend national boundaries, there are no effective international regimes or institutions that have these problems in hand. As Denis has already told us, government is struggling to manage these kinds of threats. Instead we see organizations like the World Health Organization or the International Telecommunication Union that are slow, bureaucratic, and even corrupt, struggling to remain relevant. The post-war structures that have kept relative peace for 70 years face a crisis of legitimacy as rising powers that were not present at Bretton Woods scorn the old order and create their own institutions and power centers.

Cyberspace Security and Stability

Let's start with cyberspace. You have all seen maps showing global flows of electronic information: financial and other business transactions, social interactions on platforms like Facebook, state-on-state espionage, and criminal activity. I have looked at these maps, and they look very much maps of a different, more mature network, the air traffic system.

Everyone here is painfully familiar with the provisions that keep that network secure: identity proofing of everyone who gets close to a passenger plane, licensing of pilots, filing of flight plans, certification of aircraft, etc. We have none of these things in cyberspace. Yet the financial value of the commercial transactions conducted over the Internet (and here I'm not even counting SWIFT and other special purpose networks) is actually 100 times greater on an annual basis than the value of goods transported in the air cargo system.

In commercial aviation we have organizations like the private sector International Air Transport Association and the governmental International Commercial Aviation Organization that partner to maintain safety and security on a global basis. There are no comparable institutions for cyberspace.

Finally, norms of behavior and international law apply in the airspace – it is illegal to shoot down a commercial aircraft. But in cyberspace, the applicability of international law is still being debated.

Instead, the world is in a global cyber arms race, led by the United States, Russia, China, Iran, Israel, and some European countries, with many others, including the DPRK, following close behind. Non-state actors such as organized criminal gangs and the Islamic State are terrorist groups are also a threat.

This arms race differs from the nuclear arms race of the last century. First, the good news. The scale of potential damage from even the worst cyber attack is much lower, whether measured in physical, financial, or human terms. And here it's worth noting, as James Clapper the US Director of National Intelligence did in his most recent global threat assessment, that the most devastating cyber attack would not be shutting down an electric grid, but corrupting the data that flows through the international financial system. But unfortunately, we have seen examples of both attacks in the past year, with a partial shut down of the grid in Ukraine and major cyber thefts over the SWIFT network.

Second, access to powerful cyber weapons is much easier that assembling a nuclear device. Cybercrime as a service is a vibrant industry, with weapons bazaars hosted on the unsearchable "dark web" (and on servers based primarily in Eastern Europe) and attack infrastructures, available for rent by the day and paid for using bitcoins, that can infect or disable millions of computers.

Third, the private sector is much more powerful in cyberspace than in the nuclear space. Major companies have a much greater say in what goes on in cyberspace than most sovereign states. And some of those international companies, including EWI sponsors Microsoft, Huawei Technologies, NXP Semiconductors, and Unisys, are taking seriously the responsibility that comes with such power and working with us and others to develop and promote norms of industry behavior.

Finally, in cyberspace there is a much more significant danger of miscalculation that could lead to escalation. It is very hard to tell in real time who is responsible for a cyber attack, and relatively easy for a bad actor to make it appear that an attack is coming from somewhere else.

Progress is modest. A group of governmental cyber experts has worked at the United Nations for over 10 years to come up with an initial set of non-binding norms of behavior in cyberspace.

These include:

- Not allowing the use of information and communications technology, or ICT, to intentionally damage another country's critical infrastructure.

- Not allowing international cyber attacks to emanate from their territory.

- Responding to requests for assistance from another country who has been attacked by computers in the first country.

- Preventing the proliferation of malicious tools and techniques and the use of harmful hidden functions.

- Encouraging responsible reporting of ICT vulnerabilities and sharing associated information.

- Not harming the information systems of the authorized cybersecurity incident response teams.

On the private sector side, global ICT companies are beginning to step up to the responsibility that comes with their great power in cyberspace. For example, Microsoft recently issued a set of norms of industry behavior that global ICT companies should follow in their business practices.

Examples of the kinds of norms that companies are considering include:

- Creating more secure products and services.

- Not enabling states to weaken the security of commercial, mass-market ICT products and services.

- Practicing responsible vulnerability disclosure.

- Collaborating to defend their customers against and recover from serious cyber attacks.

- Issuing updates to protect their customers no matter where the customer is located.

This progress must be accelerated in order to prevent major accidental or intentional disruptions to global economic and political stability.

I want to turn now to the enterprise threat picture.

My remarks today are supposed to be about cyber “threats.” When I worked for the US government, we would speak ironically about the “really scary briefing” that is de rigeur in conventional presentations about cybersecurity. I am not going to give you that briefing today. We are not going back to the Stone Age, or even the Pre-Digital Age, because of cyber threats. My aim is instead to give you a sense of texture of what is in fact a complex technical, economic, and geopolitical problem, with the hope that it will provide useful perspective for the next day and a half of conversations about how to evaluate cyber risk to covered entities, and to the insurance industry. A more accurate title for my remarks might be: “Risk in Cyberspace Is Full of Unknowns.”

You-all know more than I do about risk, and I hope to learn from you today and tomorrow. When I was in the government, however, we understood security risk as a function of three components: vulnerability, threat, and consequences. I will therefore start by unpacking each of those three components for commercial enterprises in the cyberspace context. I will then turn more generally to the risks this situation poses for the insurance industry.

Vulnerability

Let me begin with vulnerabilities. Simply put, these are abundant. The technology that the global economy depends on is full of them. That is why the cybersecurity community talks about interconnected digital technology as the “attack surface.”

In no other industry do the customers (or “users,” as they are called here and in the illegal drug industry) expect the level of defects that we experience with supply information and communications technology (ICT). I mean, what if every so often our cars just stopped unexpectedly in the middle of a trip, we called a mechanic, and he told us to turn off the engine and restart it? How can it be that we tolerate this behavior? And then there is the almost complete lack of liability exposure that ICT firms face, particularly in software, and which we perpetuate every time we click “I Accept.”

Clearly, the industry is at a rather immature stage. Its rapid growth in importance has outstripped systems of governance, including the first line of defense – the market. As a general matter, until very recently customers demanded two things from the firms that supply ICTs – price and features. The market has responded, giving us all manner of convenience and efficiency, in business and in our private lives. What would we be without Pokemon Go, or, frankly, Facebook. I mean, who here remembers Minitel? This is better, right? Anyway, today, buyers are starting to recognize the criticality of ICT to their daily activities, and thus they demand, and may be willing to pay for, security.

Yet there is a gap between what they need and what they are able to command. To address this gap, we recently published a “Buyers Guide for Secure ICT.! This guide recommends 25 questions that buyers can ask ICT suppliers to help them evaluate the security of the products and services that these suppliers deliver.

This is the beginning of a long journey. A large software program may contain tens of millions of lines of interconnected programming code, each of which may introduce a vulnerability because of uncorrected errors or unanticipated (or, worse, maliciously intended) interactions with other parts of the program. There are things the suppliers can do to reduce the risk of creating vulnerabilities, and these prctices are what the Buyers Guide is intended to encourage.

In the meantime, we can only fall back on aphorisms: the first, my favorite, is that there are two kinds of firms, those who have been hacked and those who know they have been hacked. It’s actually better to be in the second group. Most major attacks take six to 18 months to discover.

By then, much of the damage has been done. But at least senior management gets the idea that this can happen to them and that they need to work to reduce the likelihood of recurrence.

Denis is right that CEOs don't like to talk about this issue in public. They close the doors...but, they do not turn off their phones or leave them outside the room, so actually it is not unlikely that those conversations are being heard in various other places.

The second aphorism is: “Offense wins.” We can see the truth of this by simply reciting the names of some of the most recent US victims: Democratic National Committee, Sony Entertainment, JP Morgan Chase. Each of these organizations was paying attention, consistent with its organizational culture, to cybersecurity. And each experienced major damage that it was unable to prevent.

The Evolving Attack Surface

The situation is made more complex because it is hardly static. Rather, we face a dynamic technological environment with product cycles of 18 months or less. Let me comment on three developments that are already affecting the security picture.

Virtualization and Cloud

We are moving to the cloud. We store our information there on virtual machines operated by major providers such as Amazon Cloud Services, which accounts for more than half of Amazon’s revenues. Mixed impact on security. Better capacity and capability. More resilience. But concentrated target, potential consequences higher.

Internet of Everything

A second emerging source of risk in cyberspace is the so-called Internet of Things also referred to as the Internet of People or just the Internet of Everything. By 2020 there will be ten times more devices – such as fitbits, heart monitors, automobiles, thermostats, machine tools, and floodgates -- connected to the Internet than there are phones and computers. These devices, when combined with 3-D printing, promise to transform major industries, including transportation and manufacturing. They will also create a ubiquitous, global sensor network that will be aware of and communicating what is going on everywhere. And these devices will be shockingly insecure – build with easy to guess passwords, transmitting their data in the clear, and unable to be modified when vulnerabilities are discovered in their operating systems.

The conventional wisdom in cyber circles is that the Internet of Things represents a massive increase in the attack surface. But at EWI, we are exploring two questions. First, why do we assume the bad guys will own the sensor network? Why not have the good guys own it and use the knowledge of what is happening on the internet to increase security – for example, by isolating problems and fixing them before they can spread?

Second, we ask, how will this change the way firms invest in cybersecurity. Today firms try to update every endpoint with the latest security patch and warn employees not to open suspect attachments or click on unknown links. This not work with 5 billion connected devices. It will work even less when there are 50 billion devices. At EWI we believe there will be a shift in strategy, moving away from securing endpoints and towards greater network security, both within enterprises and also at the level of cloud service providers and telecommunications companies. I am happy to discuss some of the implications of this development in more detail should anyone be interested.

Dynamic Threat Environment

Unfortunately, innovation is not limited to the good guys. Well-funded threat actors are constantly innovating and coming up with new attack vectors. Take Ransomware. Old scenario – steal info and send email. Today, freeze the computer and hold hostage. Hospitals particularly vulnerable targets.

[A second innovation crypto currencies virtual currencies bitcoin. May have positive uses but today largely used for evil.]

What Is Being Done

Reducing vulnerability by sound cybersecurity practices

Preventing the attacker from getting in, it turns out, is impossible right now. If you are connected to the Internet, someone will get in. An attacker will find an unpatched vulnerability, or an employee will open an infected attachment or click on a malicious link. A disgruntled system administrator can compromise systems without detection. Firms can, however, limit the impact of these vulnerabilities through sound cybersecurity practices. And there are multiple guides available.

One that is gaining currency in the US is the Cybersecurity Framework created by the National Institute of Standards and Technology, or NIST, which is part of the US Department of Commerce. The framework lays out the basics of a cybersecurity program that all firms should manage to.

The EWI Buyers Guide that I mentioned earlier supplements that for firms who want to reduce risk by using technology that is less risky. EWI is also working on other elements of risk reduction.

For example, we are working internationally with the owners and operators of critical infrastructure – like power plants and chemical facilities – to share lessons learned and sound practices based on their experiences.

[i.	Business continuity

ii. Prepare to operate in degraded environment

iii. Assure Redundancy

iv. Exercise

v. Don't Connect!!]

And we are convening an international conversation designed to find the most appropriate balance to the questions posed by the US lawsuit "FBI vs. Apple" – that is, how to balance law enforcement's need for access to digital evidence with business and citizens need to protect the confidentiality of their proprietary and personal information.

Hopefully I have established that firms that use commercial ICT are vulnerable. You will remember that I think Risk is a Function of Vulnerability, Threat, and Consequence. Let me turn next to the threat part of the equation.

Threat

Let's turn now to Threats. Inside the cybersecurity culture, we talk about threat actors, malicious actors, the bad guys. These are also plentiful, and we like to talk about the "threat landscape." It's a jungle out there.

Threat has two components: capability and intent. Hercule Poirot would always attempt to understand whether a suspect had the means to commit a particular murder – capability – and the motive to commit murder – intent.

The conventional wisdom on cyber threat actors has been that those with the capability to create mass events, large scale damage, do not have the intent. And those who would like to disrupt modern life through cyber means do not have the capability. Of course like all things tech, capability becomes cheaper and more accessible every year, so reassurance is eroding. Today the cybercrime as a service industry is booming, and the market in zero days – previously undiscovered vulnerabilities that defenders have no time to prepare or – is robust. Many ICT companies are creating "bug bounty" programs, which pay security researchers to tell the manufacturer rather than sell the vulnerability on the black market. Some security consultancies also buy zero days and disclose only to their clients. And, as we saw recently in the case of NSA and Juniper, governments may discover or purchase vulnerability information and stockpile them for future offensive use.

Who are these threat actors? In order of decreasing capability they are States and their proxies, criminal syndicates, privileged insiders, non-state actors including commercial competitors, and everyone else. Earlier I mentioned some of the most capable cyber powers from an offense standpoint. Some states, Russia in particular, use proxies to achieve their offensive goals, including so-called hacktivists. These people provide a veneer of deniability, as in the case of the

2007 cyber attack on Estonia. State actors may use cyber weapons to achieve any national purpose, whether it is conventional national security espionage such as Snowden revealed, disruption of an adversary's election process, as the Russians are attempting to do in the United States, or economic espionage conducted by Chinese military personnel.

Meanwhile, the US remains the place where the most spam and cyberattacks come from. The US has the most computers and servers, and those become part of the attack infrastructure for the global set of malicious actors.

Criminal syndicates – organized crime – today use cyber primarily to fund other activities such as human and drug trafficking. The most powerful are located within or near Russia. A few Romanian towns are notorious. These groups coordinate their activities using the internet to host highly secure, closed groups that admit members based on trust established in the physical world.

Industrial competitors may use cyber tools to steal proprietary information. This is increasingly a problem between Chinese firms within China, one factor that helping focus the Chinese government on reducing its own attack activity and starting to advocate for better global cybersecurity.

While we're on the topic of non-state actors, there are of course terrorists. At the moment they are using the internet to propagandize, recruit, educate, and plan. Today they still embody the conventional wisdom about having intent, but not capability, at least in terms of cyberspace.

[v. Privileged Users (biggest)

vi. Everyone Else (carelessness, recreational hackers)]

Intent (= motive)

[i. Political – elections

ii. Military – in theater and intelligence

iii. Economic – economic espionage

iv. Financial – money laundering

v. Commercial – trade secrets and IP

vi. Other – recreational]

Types of Attacks These are not "cyber" crimes

[i. Business interruption through denial of service (Iran on banks)

ii. Breaking and Entering – (for all purposes)

iii. Trespassing (for all purposes)

iv. Fraud (and Abuse) – (for all purposes)

v. Theft – IP and money

vi. Extortion (□ Ransomware)

vii. Corruption of Data – miscalculation

viii. Destructive attacks – grid]

Countermeasures (i.e., beyond reducing vulnerability and consequences)

[i. Norms (we are working with Gov of Neth)

ii. Deterrence

1. Criminal prosecution;

2. Threat of retaliation incl. hack backs, naming and shaming)

iii. Attribution

1. (reasonable doubt, preponderance of the evidence, legal remedies)

Consequences

Alright, we have considered vulnerabilities, also known as the attack surface, and toured the so-called threat landscape. Let’s turn briefly to the third component of risk – the so-what – consequences. For ironically, it is the rapid increase in the level of possible consequences that is fueling the expansion of the threat landscape. It is much easier and safer to rob a bank online than with a machine gun. And he potential damages increase along with our dependency on ICT. If you add to this the aggregation of risk in the form of increasingly large cloud platform providers, and interdependencies and interconnection across sectors, you can come up with some scary scenarios.

For at least a decade, there has been a lot of hype that we will all be left freezing in the dark, as was the case at the turn of the 21st century with the so-called millennium bug. These scenarios have not materialized, and in fact it is actually quite difficult to create broad systemic damage today. But the capability to attempt catastrophic attacks is increasing, and the generally deteriorating international security situation does not help

In fact, to date the consequences have been relatively modest. Economic losses from cyber attacks have been estimated to amount to some $500 billion every year, although no one really knows. That is less than one percent of the global GDP. In addition to direct financial costs, there are reputational losses as with Sony Entertainment where the CEO actually lost his job, and damages to third parties, which is where privacy and data breach laws have focused. But the stock market generally yawns at even the most spectacular attacks.

I expect we will spend much of our time in the next few days discussing in some detail the exposure that individual firms are facing, and I look forward to contributing my perspective during those discussions. Therefore I am not going to dwell further on the macro consequences from cyber failures or attacks. We actually know very little about the actual or potential magnitude of such consequences, which leads me to my final topic.

Risks to insurers.

I want to conclude by spending a few minutes on the unique risks that the insurance industry faces.

For our discussion of vulnerabilities and threats focused on what we know about those elements of risk. But from an insurer's point of view, given our limited knowledge of consequences, we are talking much more about unknown risk than known risk.

There is an amazing lack of actuarial data.

The principal data we have in the US is from mandatory reports of so-called data breaches, that is the loss of personally identifiable information. Reporting thresholds vary by state in the US, but in general when the theft or inadvertent release of hundreds or thousands of records is detected, firms must report them to state regulators and to the victims. And, a fairly mature insurance business has grown up insuring the data holding companies against the costs of assisting the third-party victims.

Beyond that, there is limited information to be found in 10-Ks and other public reports. The response to a requirement to report material cyber events, levied by the US Securities and Exchange Commission, has produced a few anecdotal reports, but most firms have decided the events are not material or comply with very general language.

In some cases, reporting requirements are on the books, but the results remain confidential with the regulators or are not enforced. I was in India earlier this week discussing the lack of enforcement of a central bank requirement that banks report cyber attacks.

We are left with general estimates, such as the annual report by Verizon and the US Secret Service on the costs of cyber crimes.

Lack of Underwriting Standards

A second source of risk to insurers is the lack of generally accepted underwriting standards.

There is no “building code” for ICT manufacturer. Nor is there any officially recognized independent inspection organization that will certify their products and services. There is no professional licensing of those who write code nor of those who install and maintain the systems it runs on.

Nor is there an agreed risk management framework. Underwriters are left with a labor-intensive examination of the “security culture” of organizations or taking a probabilistic approach to policies. One bright spot in the US is the emergence of the NIST Cybersecurity Framework as a potential basis for standards. A committee made up of financial services firms has undertaken to adapt the framework to address the specific cybersecurity risks facing exchanges and clearinghouses, and this could become the basis for a standard of care that courts enforce or that regulators adopt.

But such maturity remains several years away from today, and the unknowns clearly outnumber the knowns when it comes to assessing cybersecurity risk.

EWI

Let me conclude with a pitch for the work of the EastWest Institute. As in other threat domains, EWI works to create a more stable environment, a safer ecosystem, lowered risk, and lowering potential costs to individuals, firms, and society. We are independent. We avoid taking money from governments, relying instead on donations from three sources: wealthy individuals who want to make the world a better place for their grandchildren, public foundations interested in our work, and companies who want to reduce market uncertainty and can benefit from a better understanding of the global security environment. Perhaps some of you will consider joining our community and help make the world a more predictable, and safer, place.

Thank you for your attention.