Security –
Who are the main targets, and where are the main sources of breach?

> *It is one who is thoroughly acquainted with the evils of war that can thoroughly understand the profitable way of carrying it on.*
>
> *By discovering the enemy's dispositions and remaining invisible ourselves, we can keep our forces concentrated, while the enemy's must be divided.*
>
> *- Sun Tzu, The Art of War*

When asked if companies have adequate security in place to protect their interests, industry experts often hear, "We've Got That Covered". But is this really true?

Good and evil have existed from the beginning of time. In the fast paced Internet age, malicious threats and evil manifest themselves at warp speed. Has the Internet data deluge become so overwhelming that many people have shutdown, detached, withdraw, or perhaps reached an emotional state whereby we ignore these emotions and enter what psychologists refer to as a "flat affect", whereby we have no emotions? Is the statement, "We've got that covered", an example of such a psychological response to these ongoing security threats and stressors, or perhaps a comment made without knowing the full facts?

So readers - here are some staggering facts.

Global Landscape

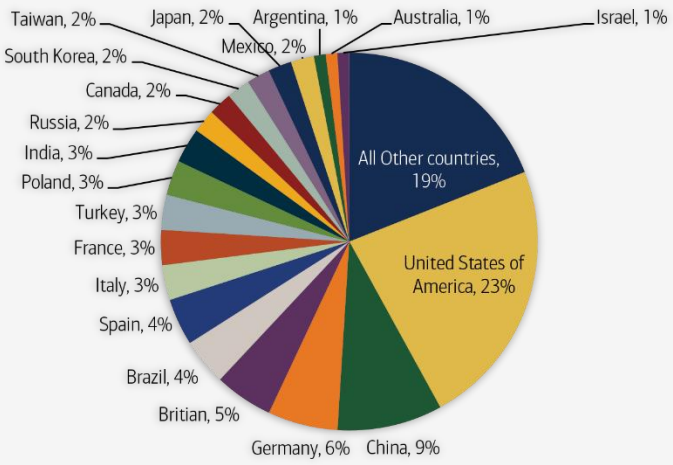
Cyber risks are one of the top 10 global risks today for government, corporations, and individuals. If current threats persist, security breaches could result in up to $3 Trillion in global economic loss by 2020. And, if technologies, processes and defensive behaviors are not adopted

quickly the losses will be even higher (WEF, McKinsey). McAfee believes close to 1 percent of global GDP is at risk. One percent is a large number in a slow growth global economy. If the 'bad guys' can steal intellectual property and trade secrets, the impact is even greater – impacting competitiveness, jobs, and ongoing macro-economic prosperity.

United States Most at Risk

Threat sources and targets are closely correlated with size of the economy and broadband Internet availability. So where are threats greatest? You probably guessed correctly - the United States. Up to 50 percent of attacks originate in the US and 59 percent take place in the US (IBM). But most networking experts know attackers leave little trace, frequently masking their origin and re-routing their attacks to a different region. The really bad guys who play in the 'dark web' know this tactic well.

Top 20 Countries with the Highest Rate of Cybercrime:



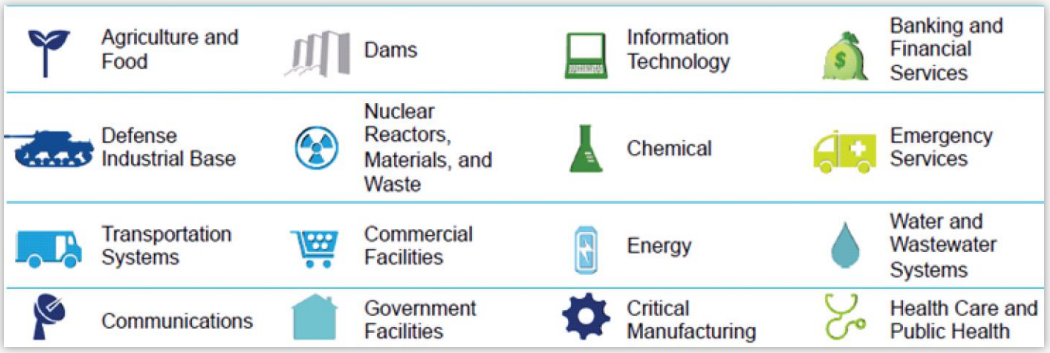
Source: Symantec

Ready yet to suit up and play on The Defensive Team? Read on.

Core Infrastructure Most at Risk

The Department of Homeland Security identified 16 core infrastructure sectors most at risk: chemical, commercial, communications, core manufacturing, dams, defense, industrial, emergency services, energy, financial, food/beverage and agriculture, government facilities, healthcare and public health, IT, nuclear reactors, materials and waste, transportation systems, water and wastewater (Deloitte).

16 Critical Infrastructures at Risk:



Source: Deloitte

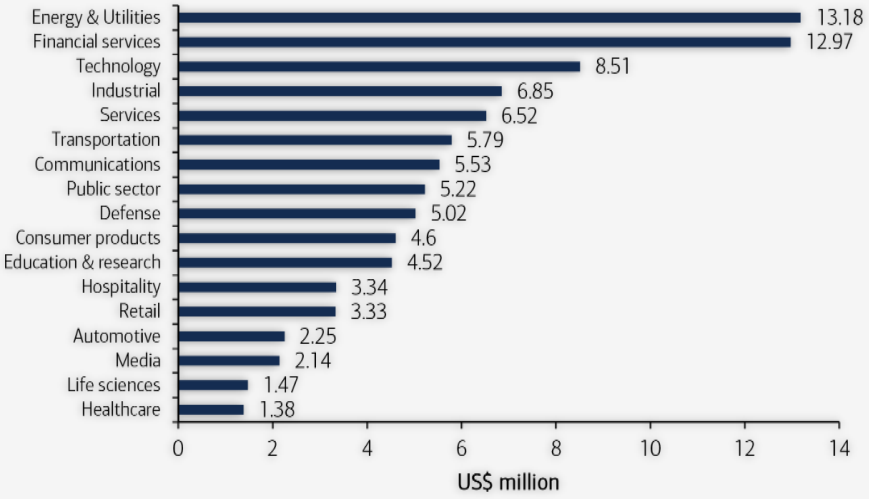
What Industries Are Most Vulnerable?

The facts, trends and threats to our security are growing exponentially. Cybersecurity risks are becoming one of the largest threats to corporations today. IBM Security Services reports approximately 250,000 incoming attacks per day, every day. Targeted, malicious, major attacks aimed at collecting, disrupting, denying, degrading or destroying information is estimated at 12,000 in 2014 (Source: IBM).

In 2014, the price of cybercrime for the average US company was at a record $12.7 Million. Companies in energy and utilities, financial services and technology were hit hardest with

greatest financial impact.

Average Annualized Cost of Cyberattack by Industry Sector (USD):



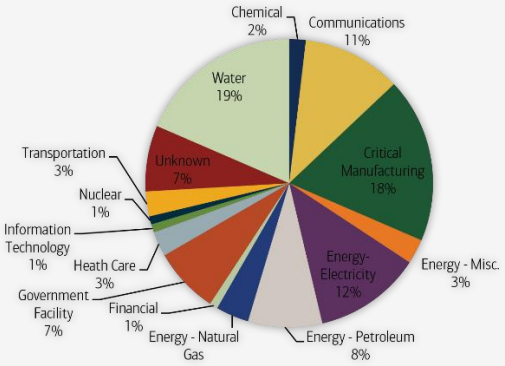
Source: Ponemon

Reported Incident by Sector

ICS-CERT (The US DHS Industrial Control Systems Cyber Emergency Response Team), charged with monitoring and responding to cyber incidents across all critical infrastructure areas, responded to 108 incidents in the first half of 2015. The energy sector reported most incidents. Importantly, regardless of industry, a large majority of incidents go unreported. Water and core manufacturing reported a combined 37 percent of incidents.

FY-15 Mid-Year Critical Infrastructure Incidents by Sector:

Source: DHS ICS -CERT



The IoT Landscape is Exponentially Increasing the Playing Field

With the estimated 50 billion smart, sensing devices estimated to go live by 2020, adoption of cloud computing, introduction of new software apps, and increased threats by the 'bad guys", the threat playing field has increased exponentially in size. Each "smart" sensor is an "exploitable" doorway into a network to a hacker. Hackers can access "smart devices", entering your car, home, your manufacturing facility, power plant, or water supply. According to HP, 70 percent of the most commonly used IoT devices contain vulnerabilities.

And it's been long understood that data networks and software are never secure. Hackers know that with the right level of motivation and force any network is penetrable.

Rapid cloud deployment, number of apps, user accounts, files, third-party data storage and management has significantly increased the threat field. The growth of corporate cloud adoption has increased the threat field 4x through collaboration via public cloud apps and third party cloud apps connected to corporate systems, and 10x for files stored in public applications. Over 100,000 risky files per organization are stored in cloud applications. Over 4,000 files per organization containing passwords are stored in public cloud apps containing credentials to corporate systems. One in 4 employees violate corporate security policy in public applications. (Source: CloudLock).

Threat Sources: Coming from the Inside

Up to 71 percent of attacks are thought to be undetected, while only 31 percent of organizations are able to uncover intrusions internally. Most attacks go unreported. Malicious actors are present on victims' networks for an average of 205 days before being detected (Source: Verizon). In 2014, "insiders" (those having either physical or remote access to an organization's systems)

are the #1 threat, accounting for 55 percent of incidents. Malicious insiders accounted for 31.5 percent and inadvertent actors 23.5 percent (source: IBM).

The DHS has seen tremendous growth in homeland security threats against nation states and core infrastructure including espionage, cyberwar fare, hactivism, and terrorism. Cyber espionage, a Sun Tzu's type approach of blending all known cyber tracts together, often perpetrated by sophisticated hackers poses the #1 threat to our core infrastructure and national security.

According to Verizon, the main data compromised by cyber espionage is secrets, representing over 85 percent.

Possible Entry Points: Backdoor through SME Partners

So for a malicious actor, the entry points are increasing. It's less likely malicious perpetrators will attempt to enter core infrastructure by going through the front gate by passing the guard but instead will enter through the weakest link, or a "backdoor" into the target. Smart (aka exploitable) sensors and the explosion of software apps and cloud computing deployment only paint a partial story.

We also know that over 80% of known current attacks are targeted at small and medium enterprises (SME), and in particular those SMEs who might be doing business with the ultimate target – perhaps within the core infrastructure, manufacturing, or target industry space. As Warren Buffet stated after the economic downturn in 2007, "it's not who are you sleeping with that matters, it's who they are sleeping with" with respect to counterparty risk. Supply chain or outside communications partners can present the same sort of risk to the larger, corporate target.

The Psychological Impact – The Trends and Day Job Decision-Making

Most realize that government and corporations perceive of such widespread risk, but many fail to realize the fear of security breach ranks #1 for individuals. Sixty nine (69%) of US residents worry either frequently or occasionally about loss of credit card information, followed by the closest second fear (62%) of having their phone or computer hacked. Interestingly, only 30% worried about their home being broken into. These same individuals perhaps work in corporations who are then charged with thinking and acting each day to the ongoing security threats at work, as well as home, creating a longer duration sense of anxiety resulting in forms of detachment to proactively address the deluge of business threats.

The threats to our core infrastructure and manufacturing are staggering. We all need to read, then re-read "The Art of War" and play on Team Defense. We need more players on the field. There's a position for everyone. The best defense is a strong offense, and the stakes are too high not to all think this way. Everyone should be on alert to abnormalities and report suspicious activities immediately, be watchful and vigilant by adhering to security policies and procedures, and implement them immediately if those procedures don't already exist. Be on high alert to abnormalities, listen to the "inner voice", and speak up. Don't retreat, and detach. But continue to learn, adapt, communicate and be engaged and proactive.