Cyber Security as an Employee Benefit

Protecting Individual Employees and Perimeter Operating Environments.

The Personalization of Cyber Risk

Like everything it touches, the Internet has successfully democratized cyber risk, and the theft of personal information has become the motive for most all cyber attacks today. This motive holds true across target size and industry sector and is independent of the final intent of the perpetrators.

Unlike IT security threats of just a few years ago, the target of attacks in modern cyber warfare is focused on individuals and their personal information including that of employees, customers, patients, vendors, and business associates. This report examines how we got here, what the future holds, and provides context, framework, and suggested measures for organizations seeking answers to the emerging security challenges ahead.

Breaches at Target, Home Depot, J.P. Morgan, Anthem, Sony, and most recently the U.S. Government by way of the IRS and OPM have one thing in common; motive. The targets are across economic segments and represent both public and private sectors. The alleged perpetrators range from Russian gangs to the Chinese and North Korean governments and militaries. Their ultimate intentions range from profit by re-sale of the information to fraud, extortion, and political agendas including social pandemonium, but their attack motives are the same: the theft of personal information. While we use well-publicized mega-breaches here for their reported facts, the common denominator of this motive holds true across the vast majority of attacks today.

How did we get here?

- The smartphone and mobile computing began the Internet's democratization of cyber risk by driving information, activity, and value to the ever-expanding perimeter environments. The mobile adoption rate far exceeds that of any other technology in the history of humanity, including TV, PC's, email, and the Internet itself. Since 2014 mobile traffic on the Internet exceeded that of the desktop and the delta between the two continues to expand.
- To accommodate a seemingly insatiable appetite for rich, ubiquitous access to data, Internet "clouds" have exacerbated the diffusion of information.
- Whether an attack is for profit, corporate espionage or politically motivated, personal information and details can provide the keys to the fulfillment of the perpetrators ultimate agenda.
- Investment in cyber security has traditionally taken place at the enterprise level, with a focus on protecting server-centric system architecture.
- Now, the richest targets are the least defended, most vulnerable to attack, and are entirely unprepared for the risks at hand today, much less the increasingly hostile environment guaranteed for tomorrow.
- Suddenly, for criminal syndicates, hacktivists, anarchists, militaries, and governments, personal information has become the cyber attack target of choice. All of these diverse organizations are re-deploying resources from traditional methods of perpetration to cyber, and the level of engineering, sophistication, and potential consequences are increasing at dramatic rates.

What does the future hold?

- Moore's Law is driving change and after a half-century of compounding, the exponentials phenomenon is kicking in. With the tipping-point being mobile computing, technology will increasingly surround our everyday lives and be part of most all of our regular, daily activities.

- IOT – The Internet of Things. By average estimates, Internet-connected device count is doubling every year and a half. The devices are increasingly “smart” and “aware”, and collect massive amounts of individual-oriented data.
- Today, the information available on the Internet doubles every couple of years. By 2020 it will be ten times what it is today, and be doubling every 72 hours.
- Datafication - Big Data software can quickly sort, sift, and mine enormous volumes of information and in the hands of nefarious parties, makes a powerful tool for data exploitation. Data is being stolen, collected, and curated for the assembly and deployment of highly engineered attacks across large volumes of targets.
- Digital currency technology such as BitCoin now provides anyone with anonymous, portable, and liquid wealth and is driving crime for profit to the Internet. IBM is creating a digital cash and payment system that will give the same attributes as bitcoin to all major currencies in the world, but without the need for bitcoin itself.

The Internet is the platform for crime and warfare of the future, and personal information is at the center of its exploitation.

Individual user’s and perimeter environments hold the greatest risk.

Now, the greatest threat lies not with a “Cyber Armageddon” scenario taking place within IT managed, server-centric architecture, but with individual users and the fringe, or perimeter environments of the network, where individuals increasing engage online. According to a threat report by Intel, low-level online extortion attacks nearly doubled in the first quarter of 2015 and in February the U.S. Director of National Intelligence, James Clapper, declared the “low-to-moderate” threat environment to be the primary risk at hand.

"Rather than a 'Cyber Armageddon' scenario that debilitates the entire US infrastructure, we envision something different. We foresee an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time, which will impose cumulative

costs on US economic competitiveness and national security." ***James Clapper, Director of National Intelligence.*** *"Worldwide Threat Assessment of the US Intelligence Community" presented to lawmakers on Feb. 26th, 2015.*

A New Approach

While investment in defensive technology is still a pre-requisite, the personalization of cyber risk requires an application of the social sciences to surviving in the digital age. Individual awareness, behavior, and accountability need to be addressed and applied beyond the workplace by integrating best practices into our everyday lives to bring the change necessary to counter the mega-trends of risk facing the enterprise today.

From a cyber security standpoint, a perimeter environment includes any location where information technology is not directly monitored and managed by the IT department. It can include remote offices and branches, personal residences and vacation homes, mobile locations, and public networks.

With these concepts in mind, we make the following recommendations:

1. The IT department can't solve or sufficiently mitigate the problem alone, and requires partnership across the organization.
2. Buy-in is required across the organization and visible leadership and support from the top down are necessary to inculcate necessary change and adoption.
3. Firm wide, training must go beyond the enterprise and IT-centric view, and address the issues from an individual's standpoint for empowerment beyond the workplace to enhance effectiveness, buy-in, and long-term retention.
4. Treasury knows where the assets are, who accesses them and how, and the department can be especially beneficial to a collaborative partnership with broad, organizational risk-control functions.

5. Analyze the perimeter environments and be concerned with remote locations, mobile users, and the supply chain as potential weak points in the system. Think about people and how they connect at the perimeter to add additional security measures at that juncture.
6. Have a plan with roles and responsibilities especially as it pertains to the reporting process of an attack or breach.
7. Follow newly emerging innovation in the cyber security industry. After decades of stagnancy, fresh investment capital has been stimulated by the privacy and information security regulatory environment and increasing consumer awareness. A new wave of entrepreneurs is disrupting the industry with innovative solutions that are becoming increasing effective and user-friendly.
8. Invest in the protection of your employees' homes and families from cyber risk.

#8 on our list of recommendations may be the most economically rewarding measure a firm can take, and is a direct application of the social sciences requirement to effective defenses today. Additionally, it can play a distinct role in optimally positioning the enterprise for managing the risks of the future.

Protecting Your Employees' Homes and Families From Cyber Risk

The delta, or chasm, between hyper-changing technology and its users' (us), is going parabolic, and the phenomenon lies at the core of our challenges. Without focus, apathy is assured. Approaching cyber risk holistically puts the individual at the center of the solution, significantly raises awareness, and increases the individual's application and retention of safe practices.

Today, cyber risks that the enterprise and employees face in the workplace are the same risks individuals face in every other aspect of their daily lives. For all, technology has become "mission critical" to regular, productive activities. Partnering with your employees to address the issues by focusing on individuals, as opposed to

exclusively focusing institutionally, and addressing cyber security as a lifestyle, applicable across employees' roles and responsibilities both personally and professionally, can provide the impact and ROI needed for increased effectiveness.

When considering training, tools, and solutions for addressing the personalization of cyber risk and the vulnerability of individuals and perimeter environments, we recommend an approach based on four fundamentals.

Protect the Device – Smartphones, laptops, pads, tablets, and about anything that connects online should be protected using state-of-the-science device protection solutions. Fortunately, recent innovations have brought high-quality and effective protection systems that once were available only to large, server-centric networks, and made them available to individuals and their devices to function securely in all environments and over any networks.

- Device protection should include remote management features that eliminate the need for user-input or behavioral modifications.
- Real-time antivirus, browser and application protections, and the host of defenses standard with most high-quality solutions, are essential.
- Lock and Erase functions are optional.
- Password management applications should work seamlessly across mobile device platforms, and the enterprise should sponsor software purchases and training for all employees.
- Automatic updating and patching of operating system software and other, vulnerable 3rd party applications such as Adobe and Java.
- Increasingly, collaborative threat intelligence resources are coming to bear for real-time, preemptive defenses.
- Algorithms will increase in effectiveness and application to predict and defend from future threats as they morph and evolve.

These automated and remotely managed functions will dramatically mitigate the risk of attacks to individuals and their devices, regardless of location.

2. **Protect the Connection –** Once the individual device connects online, more defenses are required to protect the information transmitted over the Internet.
    - In addition to device protection, each individual device should have a VPN, or Virtual Private Network, for automatic encryption of Internet traffic. A good VPN will protect the user's identity, location, browsing, shopping, banking, and all information transacted online, including over public WiFi networks.
    - Consumer level or "retail" VPN services have to-date been clunky to use and unpredictable in their operation. Recent innovation and new distribution models are providing much better performance and experience, and the improvements are expected to continue to improve over the near future.

3. **Protect Email Communication –** In many cases, email is the "barn-door" for personal information. Unfortunately, especially in the U.S., email is expected by many consumers to be "free" and has distracted us from some of the basic notions to the value of privacy today.
    - Pay or subsidize the cost for a private email service for your employees and families.
    - Use a service that automatically strips IP location and metadata information from individual emails as they travel the Internet.
    - Use services that employ open-source software for ultimate security, portability, and compatibility across technology architecture and platforms.
    - Private email accounts can act as multi-generational digital domains for your employees and families, and

provide a cyber-safe respite from online risk for decades to come.
    - This simple employee benefit can act as a distinct and meaningful measure for the enterprise to increase loyalty and support on behalf of the employee and her family.
    - Private email as an employee benefit communicates full engagement of the enterprise and its leadership to every individual, inside and out of the organization.

4. **Protect and Backup Electronic Documents and Files –** Remote backup services are easy and cheap, and the convenience of the cloud is great, but critical documents deserve a digital vault.
    - For scanned passports, social security cards, birth certificates, wills, trusts, tax returns, and the other documents that are core to our personal lives.
    - Easy-to-use but highly secure digital vaults act as a safety-deposit-box for sensitive documents.
    - Bringing digital document protection awareness to the employee's home and personal life increases productivity and security at the enterprise. The employee and her family will gain awareness, context, and skills that transfer across personal and professional functions.

Subsidizing the protection of these four fundamentals across your employee's personal lives will drive increased cyber security compliance and effectiveness across the enterprise. All of these solutions are highly affordable, do not invade anyone's privacy, and will provide an ROI that pays by reducing risk and increasing productivity for many years to come. Additionally, this approach to cyber security strategy positions the enterprise for optimal benefit from the forthcoming acceleration of disruptive innovation in the IT security industry.

SECaaS, or Cyber-Security as a Service, will increasingly come to play in defending individual devices and mobile environments, and solutions will be sold as subscription-based "outcomes", as opposed to "boxes" sold transactionally.

Cyber security is a paramount concern at every level of society on the planet. Unfortunately, especially in the U.S., privacy has been traded for “free” and as a result we live in a “stalker economy”. The lack of a broad, individual level of regard for personal information, and the actual value at the aggregator’s level has created a spread so wide that the economic arbitrage has fueled the creation of history’s greatest fortunes over relatively very short periods of time. It will require broad, institutional support to bring a change in mind-set for greater awareness and appreciation for the new age of risk we face.

Any corporate leadership interested in leading the enterprise toward increased levels of cyber security must align strategy and investment with the issues as they apply to individuals, the perimeter operating environments, and the everyday activities of people in their personal lives. Cyber risk will never be eliminated and will look cat-and-mouse, or whack-a-mole for a long time. However, the risk can be managed and significantly mitigated especially with new, individual-defined thinking, innovative technology solutions that work in perimeter environments, and the application of the measures across our personal and professional lives.

Brad Deflin

June 14th, 2015