Testimony of David Wagner, President of Entrust

Before the U.S. Senate Committee on Commerce, Science, and Transportation

March 26, 2014

I am David Wagner, president of Entrust, a leader in identity-based security software systems and solutions. On behalf of Entrust, we appreciate the opportunity to testify today.

At Entrust, a wholly owned subsidiary of Datacard Group, we secure and protect digital identities and information. We serve more than 5,000 organizations, spanning 85 countries, by safeguarding enterprises, governments, financial institutions, websites and citizens – including your constituents.

For its part, Datacard is the world leader in secure identity and card personalization solutions. Most payment cards in circulation today are issued using Datacard systems. As a combined company, and as a result of the ways in which we serve our customers, we possess a unique perspective on secure identity and trusted transactions and the increasing threat of cyberattacks on networks and systems.

Just more than two years ago, we testified before a U.S. House of Representatives Energy and Commerce Committee subcommittee on this same subject of cybersecurity. We said then that cybercrime poses a greater threat to the security of nations, corporations and individuals than ever before. We noted that the threat had moved from one of hacking for honor to one of hacking for harm and profit via overt criminal activity.

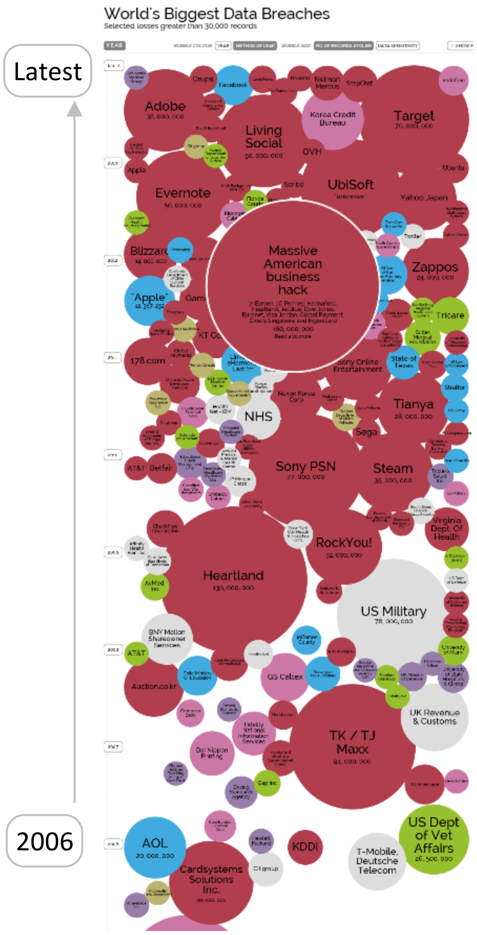
Today, it's no secret. The situation has worsened. Incidents involving the loss of personal information have increased an average of 40 percent in each of the two years since we last testified.[1] Practically every day, new headlines appear about a data breach at a financial institution, a retailer, a university, a hospital, a government agency – and the list continues.

In February, cybersecurity firm Hold Security said it uncovered stolen credentials from some 360 million accounts available for sale on cyber black markets. It also

[1] "Incidents Over Time: 2011 versus 2012 and 2013." Open Security Foundation n.pag. Data Loss Statistics. Web. 24 Mar 2014. <http://datalossdb.org/statistics>.

reported the criminals are selling some 1.25 billion email addresses.[2] The breaches impact consumer confidence and have economic consequences.

- In the US alone, the direct and indirect impact of identity theft totaled $24.7 Billion (USD).[3]
- According to the Bureau of Justice Statistics, 7% of Americans aged 16 and older fell victim to identity theft in 2012. Of these, 22% fell victim more than once.[3]
- The median loss for those victims to identity theft was $2,183, with a mean of $300.[3]
- In a report from the Federal Trade Commission (FTC), which consists of formal complaints registered with law enforcement, the FBI, Canadian counterparts, the FTC, and several other organizations, identity theft remained the largest single consumer compliant category in 2013.[4]



It also appears that the number of larger breaches is increasing. Unfortunately, and a point we will elaborate on later, there is no national breach law and the means of assessing an aggregated view of this data remain somewhat elusive.

However, one view of the data behind the breaches is shown in the adjacent figure, which is an aggregation of data from several well-known breach reporting sites.[5]

[2] Finkle, Jim. "360 million newly stolen credentials on black market: cybersecurity firm." Reuters [Boston] 25 02 2014, n. pag. Web. 24 Mar. 2014. <http://www.reuters.com/article/2014/02/25/us-cybercrime-databreach-idUSBREA1O20S20140225>.

[3] Harrell, Erika, and Lynn Langton. United States. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. 2013. Web. <http://www.bjs.gov/content/pub/pdf/vit12.pdf>.

[4] United States. Federal Trade Commission. Consumer Sentinel Network Data Book for January-December 2013. 2014. Web. <http://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2013/sentinel-cy2013.pdf>.

[5] Quick, Miriam, Miriam Hollowood, Christian Miles, and Dan Hampson. "World's Biggest Data Breaches: Selected losses greater than 30,000 records." Information Is Beautiful. N.p., 31 Dec 2013. Web. 24 Mar 2014. <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>.

What this data suggests is that the overall volume and numbers of large attacks continue to increase. Additionally, the majority of attacks are dedicated efforts to extract information (versus accidental losses). In total, it appears that both the number of records exposed and the number of incidents have nearly doubled since 2011 and the majority of these incidents were in the U.S.[6]

We are witnessing massive growth in the volume of transactions, amount of data and number of devices connected online. This attracts criminals and provides vectors for attacks. It is at the center of the rising tide of cyber issues and the increasing impact of related breaches.

The challenge is to make sure that success in protecting the growing volume of data doesn't unnecessarily hinder users from receiving the benefits of emerging technology or burden those charged with securing the systems. As policymakers, you are charged with facilitating commerce and ensuring an optimal structure for finding this balance.

The Focus: Identity and Malware

Before recommending actions to enhance our cyber posture, I'd like to provide a bit more background on how the attacks are occurring.

Although Entrust has no direct relationship with any of the victims of the December 2013 point-of-sale (POS) attacks, we can provide general insight to the attacks from public information and from our understanding of how cyberattacks are normally perpetrated.

In many of the retail breaches, and not unlike attacks witnessed in other industries, criminals are using a combination of social engineering and technical tools, such as malicious software or "malware," to steal credit card numbers and personal information.

The traditional approach to network security continues to put significant focus on developing a perimeter around the corporate network. Whether or not these defenses can be breached directly, we can ascertain that they aren't the weakest link in the defense by assessing the successful attacks. Instead of trying to breach perimeter defenses directly, criminals are focusing on obtaining an identity that provides access directly inside the network.

[6] "Data Breach QuickView: An Executive's Guide to 2013 Data Breach Trends." Risk Based Security & Open Security Foundation, n.d. Web. 24 Mar 2014. <https://www.riskbasedsecurity.com/reports/2013-DataBreachQuickView.pdf>.

The logic could work something like this: criminals know that many organizations still treat the internal network as being protected by the perimeter (i.e., castle walls and moat analogy). As a result, less attention gets paid to internal systems and where monitoring occurs, it tends to get less attention than the external environment.

As a criminal, if you can get inside, your objectives become much easier. So, what is the easiest way to accomplish this goal? A direct attack is possible against the perimeter, but this is where we're focusing our security investment and attention.

Back to the castle analogy, the walls are formidable, and the moat is deep. However, organizations are people; people working on the trusted "inside" of the network, people just trying to get their jobs done (we will come back to this later). And we generally trust these people. They become the vector for many of the attacks.

If a criminal can get one of their identities, or more specifically credentials, they have bypassed the perimeter, the walls and the moat. This can be done through social engineering an unsuspecting individual with legitimate access to the network (e.g., an employee or contractor), by exploiting flaws in a technical implementation, or via direct access through a knowing accomplice on the network.

Using stolen credentials, the criminal has virtually become "someone" on the network and appears as a legitimate user, making them difficult to see and detect. From here, the attacker can move more easily within the network, using the systems available to the legitimate user and bringing in their own more malicious tools.

How Hackers Do It

A cyberattack is typically not a single event. Regardless of the attack goal, there are a series of objectives that need to be completed along the way. As described above, each step is made significantly easier if the attacker possess the identity of a legitimate person or device on the target network.

Disciplined cyberattackers do not need to 'hack' or 'break' a computer system in order to take advantage of it maliciously. Attackers will use the system as a whole, by taking full advantage of the way that PCs and networks are engineered. PCs and their operating systems are designed to be highly connected and interoperable in order to provide excellent user experiences for their legitimate users.

This, unfortunately, also provides rich functionality for an attacker. Computer networks are naturally trusting by their nature, and cyberattackers take full advantage of that. It is very difficult to tell the difference between malicious and legitimate behavior on a PC or on a computer network. This is because the cyber attacker has stolen a legitimate identity. The attacker is not a masked, highly visible criminal. The attacker has your identity and is imitating you.

Employees inside a corporate network can be tricked into opening emails that contain a malicious payload. The original Greek 'Trojan Horse' is a good analogy, but instead of a wooden horse, the gift may be an email that looks like a legitimate request for assistance from your boss.

Anyone can be tricked into opening that email or browsing to a Web link. The email or Web link will contain the malicious payload that will infect the employee's PC, which will serve as a beachhead from which the attacker will perform subsequent steps in the attack.

By infecting the first PC, the attacker has assumed the identity of the employee on that PC. If the employee happens to be an administrator, which is all too often the case, the attacker will also have the rights of an administrator and allow the attacker to move even more quickly to their target.

The initial infection will be invisible to the employee. Attackers are using techniques that defeat end-point protections and continually adapt to monitoring. Unfortunately, most defenses at the PC and network level are based on catching attacks where the patterns of attacker behavior have been seen before. But attackers are capable of adjusting their tools and behavior just enough to slip through these defenses.

From the beachhead of the initial PC infection, the cyberattacker will use the first stolen identity to gather information on the target network and begin to move towards the ultimate target. The fog of war is quickly cleared for the attacker as they map out the network.

If you have ever browsed for a printer on an enterprise network, your own computer has performed network reconnaissance indistinguishable from the activity a malicious attacker needs to do to map out your network. This means that the attacker’s movements in your network are exceedingly difficult to distinguish from a normal user, unless you have very tight controls over identity, and the rights that those identities have.

A human resources employee should normally never need to view computer resources that store highly valuable intellectual property. A third-party partner or vendor who has been given access rights to a corporate network should not have access to anything beyond the limited systems needed to complete their tasks.

Preventing Data Breaches

You can see from the attack scenario that the criminals must be knowledgeable of the systems involved and typical responses from the compromised organization. They are knowledgeable, but they aren’t overly sophisticated. They merely use stolen identities to access and use the normal IT tools of the victim in conjunction with malware.

Although the most advanced and persistent attackers can breach even strong defenses, good security governance and strong security policies, processes and implementation can thwart most attacks or at least limit their impact.

In addition to industry standards such as the Payment Card Industry Data Security Standard, best practices for information security are covered in a number of security frameworks such as SANS 20, ISO 27002, COBIT and recent publications from NIST.

The SANS Top 20 Critical Security Controls is an example of the focus areas provided in the frameworks. The controls discussed by SANS are a subset of a larger body of work provided in NIST SP 800-53, with the top 20 controls as follows:

Top 20 Critical Security Controls - Version 5

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Malware Defenses
6. Application Software Security
7. Wireless Access Control

8. Data Recovery Capability
9. Security Skills Assessment and Appropriate Training to Fill Gaps
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11. Limitation and Control of Network Ports, Protocols, and Services
12. Controlled Use of Administrative Privileges
13. Boundary Defense
14. Maintenance, Monitoring, and Analysis of Audit Logs
15. Controlled Access Based on the Need to Know
16. Account Monitoring and Control
17. Data Protection
18. Incident Response and Management
19. Secure Network Engineering
20. Penetration Tests and Red Team Exercises

Examples of the rationale behind some of this guidance are provided below:

The principle of ‘least privileges’ should be considered a vital part of policy, leading to a minimal usage of administrative credentials. Employees and third parties are often given too many rights on a corporate network, which increases risk. If an attacker is able to steal an administrative identity, this brings huge risk. Therefore, administrative identities should be used minimally and secured strongly.

It is difficult or impossible to defend a computer network without an inventory of resources. This includes desktop computers, back-office servers, Wi-Fi and wired access points. This is required in order to create secure network architecture.

A trained security staff equipped with tools is needed to operationalize that defensive posture.

For example, an important tool to thwart identity-stealing is strong second-factor authentication. Most people think of authentication as being only username and password. Username and password is a single-factor authentication. In other words, the attacker only has to steal one secret (the username and password) in one place in order to steal the identity and be able to log in to a computer system.

Second-factor authentication requires a user to use two secrets. Strong forms of second-factor authentication exist that take advantage of mobile devices. Strong second-factor authentication provides a very high level of identity protection, not only for employees on a corporate network, but also for third-party users of the network such as partners and vendors.

Strong second-factor authentication also makes it more difficult to inadvertently ‘share’ a credential with a co-worker. Imagine a scenario where an ‘insider’ wishes to sabotage a network for malicious purposes. If an insider simply stood over the shoulder of an administrative co-worker and learned the username/password, they could simply log in as their co-worker and perform malicious activity with the co-worker’s identity. With strong second-factor authentication, this is not possible.

Complementing the above, network segmentation is a concept where important resources are only made minimally accessible to computer systems that have a need to reach them.

Focusing on the December 2013 attacks, whitelisting the software programs able to run on the POS terminal make it more difficult to install the malware. Whitelisting is a technique that allows only a specific set of software to be installed on a computer. If malware is installed on a computer, it will not match the ‘whitelisted’ set of software and be rejected.

In addition, carefully monitoring network traffic with intrusion detection and intrusion prevention systems (IDS/IPS) could allow security analysts to detect the unauthorized network traffic patterns used by the attackers.

Although attackers are knowledgeable and persistent, there are ways to reduce the likelihood of a successful attack and mitigate damages. It is commonly understood that security in layers and defense in depth help combat attacks.

However, what is appropriate for any given organization is typically defined through an assessment of risk. Inputs to this process come from the core values of the business and require top-level engagement to be accomplished successfully.

Challenges and Recommendations

One of the questions we should be asking is, “with all of the knowledge, guidance and standards, how did the breach happen?”

One avenue to explore is the pace at which we bring lessons learned from the experts on the frontline of cyber into practice. Nothing in the breaches was new. We don’t have a gap in understanding the attacks currently being executed.

Any security practitioner will tell you that good information security requires investment in people, process and technology applied consistently over time. But have we established a cybersecurity system and culture that inherently evolves at the same rate as the threats? Is the bureaucratic process seen in government and industry groups inherently too slow to adapt? If so, there is no silver bullet in technology will help.

Another problem with many cybercrimes is that the loss has an asymmetric impact on its victims. For example, although a retailer is breached, the bank bears the cost of the stolen card data, financial institutions bear the cost of card re-issuance, and consumers suffer the pain of changing cards and cleaning up accounts.

A major focus of the guidance and regulation that exists today is based on the organization conducting a risk assessment where one of the first steps is to assign value to the data. But if the impact of a breach is only partially born by the organization conducting the assessment, then the amount of protection given to that asset may not completely capture its systematic value.

Over the past decade we have significantly advanced our understanding of the threat landscape and best practices. What the most recent events are showing us is that there are opportunities to improve the translation of understanding the threats into mechanisms that turn this understanding into action. Evolving our approach and defense posture needs to be a Federal priority and we need to move forward now.

We should start with harmonizing breach notification laws so that enterprises and consumers alike know what is expected of them. The first state-level breach notification law was enacted in California in 2002; today, 46 states have similar laws.[7] However, we are still without a common federal approach. Federal harmonization of breach notification laws is a good place to start.

Second, the Federal government needs to continue to foster the adoption of best practices across both the public and private sectors. Investments in federal programs like HSPD-12 and the Transportation Workers Identity Modernization program are advancing the security infrastructure and generating significant lessons learned. NIST is also playing a key role in generating recommendations and guidance based on cross-sections of best practices and lessons learned

[7] "State Security Breach Notification Laws." National Conference of State Legislatures. N.p., 21 Jan 2014. Web. 24 Mar 2014. <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

from many industries. So, there is a good baseline to work from.

Finally, we must change the cybersecurity culture. Enterprises – large and small, public and private – need to embrace information security governance as a core responsibility. Industries where data has been viewed as a critical asset of the organization have found ways to integrate this into their DNA with many good examples existing in finance and the defense and intelligence communities.

However, in these cases, the value of the data is obvious. Losses are not asymmetrical. We may want to look closer at how industries where handling data, especially personally identifiable information (PII), is a byproduct and not an objective of the organization. Healthcare, retail and critical infrastructure are all very good examples.

In either case, we believe the focus should be on 1) how to accelerate the cycle from learning to implementation and 2) ensuring that the asymmetric nature of data is taken into account in cyberstrategy. Whether you want to drive adoption via incentives or directives is a public policy matter, but however we proceed, we need to proceed now.

Conclusion

Simply as a result of more transactions, data and devices going online, and without changes to the security posture of our most important industries and infrastructure, cybercrimes will continue to increase in frequency and potency. The asymmetric impacts will afflict those entrusted with sensitive data and the consumers, citizens and employees who put their faith in these systems.

Given the current situation, you must not let the perfect become the enemy of the good. The recommendations put forward would increase visibility into the threat environment and costs borne by individuals, organizations and the system as a whole. This insight needs to quickly filter into a more accurate assessment of risk and a system that is quicker to adapt.

Finally, the recent breaches have brought more attention to the cyber challenges we face today. We must take advantage of this focus, turn a negative into a positive, and move forward with policy that helps organizations embrace information security governance as a core responsibility. I urge you, your colleagues and the Administration to not let 2014 conclude without adoption of some measures that will better protect our economy and security.