

**TESTIMONY OF  
A. BRYAN SARTIN  
VERIZON COMMUNICATIONS**

**BEFORE THE  
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS & CONSUMER CREDIT  
COMMITTEE ON FINANCIAL SERVICES  
UNITED STATES HOUSE OF REPRESENTATIVES**

**ON  
“CYBER SECURITY: THREATS TO THE FINANCIAL SECTOR”**

**SEPTEMBER 14, 2011**

Chairman Bachus, Ranking Member Frank and members of the Subcommittee, thank you for the opportunity to testify today on cyber threats to the financial services sector. My name is Bryan Sartin and I am the director of Investigative Response for Verizon. I have been closely involved in the information security space for more than 15 years, with a particular focus on assisting both commercial and government entities in responding to cyber-related attacks.

The Verizon Investigative Response (VZIR) group handles all digital forensics, computer incident response, electronic discovery and information technology (IT) investigations requested by Verizon customers. It is a specialized team of IT investigators, hailing from four primary backgrounds: law enforcement, military, systems engineering and institutional IT. We maintain a full-time presence in 14 countries and handle more than 200 cases each year, including a significant percentage of the investigations behind many of the world’s most publicly visible data breaches.

Much of the key risk and threat related findings stemming from VZIR casework is documented in an annual publication known as the Verizon Data Breach Investigations Report (DBIR). This year’s study, released in March, was published jointly by Verizon, the United States Secret Service, and the Dutch National High Tech Crime Unit. This study encompasses more than 1,700 data breaches, over seven years of research, and more than 900 million stolen records. This is a study of security failures and the lessons that can be learned from them.

Based on my industry experience, my duties as head of the VZIR team, and as a co-author of the DBIR, I want to offer the following points for the Subcommittee's consideration:

- Although the consequences of cyber attacks may differ depending on the target, there is little variance in cyber risks and threats by sector.
- While cyber threats continue to evolve rapidly and can be executed at the speed of light, in reality most cyber crimes are typically not complex, sophisticated or fast moving.
- While there is no panacea for the prevention of a breach, the most fundamental security controls make the most effective countermeasures.
- Many businesses and other entities that are data breach victims fail to rapidly recognize and react to the lead indicators of the cyber attacks committed against them.
- Affording cyber victims some protection from litigation, fines and penalties will encourage cooperation with law enforcement, will promote successful criminal prosecutions, and will likely reduce the overall numbers of electronic crimes.

Before exploring each of these points in greater detail, I would like to provide the Subcommittee with some background information that illustrates where the VZIR team fits in the overall Verizon network security program.

### ***Securing the Verizon Network and Keeping Customers Safe***

As a provider of communications services, Verizon manages thousands of voice, video, and data networks at the local, regional, national, and international level. Our data network spans six continents and reaches customers in more than 2,700 cities and 150 countries. We serve tens of thousands of businesses and government agencies, including 97% of Fortune 500 companies and roughly 10 million residential broadband customers here in the United States.

As a large corporate enterprise and provider of communications services, Verizon engages in a wide range of activities to enhance cyber security for ourselves, our customers, and other users of our network. These activities take place at many different layers within our organization. For example, we work closely with our vendors so that their products are able to meet our security architectures and requirements. In addition, Verizon's network security group invests in a variety of tools, security sensors, and other technologies to identify and mitigate threats in cyberspace as they are emerging. Every day, we find and remove spam, phishing, denial-of-

service and other malicious activity that threaten to disrupt our network or our customers' use of it. We help customers secure their networks and data by offering managed firewall, intrusion detection and prevention, and encrypted virtual private networking services. We also offer security consulting, network analysis, incident response, and computer forensics.

It is this latter function — customer-facing security consulting, network analysis, incident response, and computer forensics — that is handled by the VZIR team, and the 2011 DBIR that I co-authored is an example of our activities in this area. This report uses an information-sharing framework called Verizon Enterprise Risk Incident Sharing (VERIS), which Verizon developed and has published as an open-source initiative. The DBIR report also provides valuable advice and guidance for corporate and government entities on tangible, effective steps they can take to better secure their networks today. Financial services firms are among the beneficiaries of the information we make available.

I would like to now offer more detailed information regarding the five points I identified earlier.

### ***Little Variance in Electronic Crimes Risks and Threats by Sector***

The 2011 DBIR shows that Hospitality (40%), Retail (25%), and Financial Services (22%) represent the top three sectors in terms of data breach victims. Cyber criminals are after data they can easily convert into cash. More than 90% of all electronic crimes included in the 2011 DBIR are financially motivated in nature.

Retailers and financial services entities tend to have the largest quantities of the data types most frequently targeted. Our research shows that the kinds of data that cyber criminals most frequently target are payment card records, such as credit card, debit card and PIN information. That was true in 78% of more than 1,700 cases. Authentication credentials, such as usernames and password combinations, are the second most frequently targeted at 45%. Other types of personally identifiable information or PII are third at 15%<sup>1</sup>.

For this reason, these entities have been and will likely continue to be key targets of electronic crimes, as will small- to mid-size businesses that handle similar data types but in lower quantities and have less developed information security countermeasures.

It is not entirely true, though, that these sectors face a unique cyber security threat landscape as compared to other sectors or industries. There is a misperception that cyber security risks and threats are sector-specific and unique. Financial IT security experts, for example, are often

---

<sup>1</sup> Note that any single data breach may show many different types of stolen records.

quick to dismiss intelligence drawn from other sectors under the presumption that no applicable lessons can be learned. That's a critical mistake. Similarly, American companies can learn much from intelligence drawn from data breaches affecting foreign entities. Our research and experience shows that cyber risks and threats are not unique to sectors or even geographies.

To the extent that subtle differences exist, these tend to manifest in organized crime rings that prefer specific language sets (e.g., Japanese versus English) or have insider knowledge of certain companies or industries. Cyber threats vary by the kinds of data that a given entity stores, handles or transmits, as opposed to varying by industry, sector or geography. Thus, cyber crimes taking place in foreign jurisdictions, as well as those targeting victims in other sectors, present applicable and compelling IT intelligence. This point particularly applies to governments, financial services, retail and hospitality companies. Hard lessons cannot be dismissed on the grounds those lessons were learned by someone else.

### ***Cyber Crimes Do Not Require Great Complexity or Sophistication to Succeed***

Electronic crimes generally do not involve complexity or innovation on the part of the perpetrators. The 2011 DBIR shows that nine of the top ten hacking methods employed in electronic crimes over the past seven years are very simple in nature. Best-in-class information security often reflects a "defense in depth" practice and avoids reliance on just one mechanism – such as a password – to secure functions or assets. Consider the following:

- Exploitation of default or easily guessable credentials accounts for 67% of cases and 30% of stolen records. Many devices often ship with default user names and passwords—such as "admin" and "password1." If not changed, use of these pre-existing default credentials offers cyber thieves an easy entry point.
- Brute force and dictionary attacks account for 52% of cases and 34% of records. We are all familiar with systems that lock-out users after some number of failed login attempts, but failure to implement such mechanisms can enable criminals to use automated tools to try vast combinations of usernames and passwords in rapid-fire succession, often leading to successful access to the system.
- Usage of stolen login credentials accounts for 21% of cases and 21% of records. For example, a criminal could purchase user account names and passwords and utilize that information to obtain unauthorized access to a victim entity from across the Internet.

- Exploitation of insufficient authentication accounts for 10% of cases and 21% of records. An example of this could involve a criminal attempting to obtain unauthorized access across the Internet to an application run by a victim entity and then finding that no login is required.

Unlike cyber threats on the Internet, where fast-moving worms or viruses can quickly propagate across vulnerable systems in a matter of seconds or minutes, actual criminal activities targeted at infiltrating and extracting data from end-user organizations do not appear to be becoming more complex or sophisticated, faster moving or more pervasive, at least not based on the data breaches that we've investigated. If anything, the techniques being used to infiltrate and exploit identified end-user data systems are evolving toward the less complex and commoditized.

In 2010, VZIR group, the United States Secret Service and the Dutch National High Tech Crime Unit investigated more unique data breach events than in any prior year. Remarkably, only five patchable vulnerabilities were found exploited.

An application or computer system vulnerability is considered "patchable" when it is known to be problematic and its discovery is followed by the release of a fix or patch addressing that vulnerability. This suggests that criminals do not need to exploit application and computer system vulnerabilities when easier pathways of unauthorized access exist, such as those listed above. Stated another way, our research shows that with so many weak and easily exploited targets of opportunity available, great complexity and sophistication are not necessary for cyber crimes to succeed.

### ***Fundamental Security Controls are the Most Effective Countermeasures***

Our research suggests that most electronic crimes could be more easily prevented than most anticipate. If the tools and tactics employed by criminals are increasingly basic, even commoditized, then indeed the most effective countermeasures are similarly simple. The 2011 DBIR shows that 71% of initial points of entry in international electronic crimes traverse remote access facilities in use by the victim entity. Remote access refers to virtual private networks (VPN), remote control and remote node applications in particular. These are remote access facilities made available to mobile employees and external IT support vendors. Of these, local remote screen sharing applications such as remote desktop and *PCAnywhere* account for 64% of avenues of intrusion. Online session screen sharing, such as *LogMeIn*, *Go2Assist*, and *NetViewer* account for 5%. Remote shell applications such as *SSH* and *Telnet* and Web-based terminal applications such as *Citrix* and *Microsoft Terminal Services* account for 2% each.

Our research does not indicate that there are systemic security flaws in these applications. Instead, the underlying problems stem from the manner in which these applications are deployed and configured by the victimized entity. Most remote access points of entry found in electronic crimes investigations tracked by the DBIR could have been prevented if the targeted remote access facility or application required a second factor for authentication. For example, if these remote access facilities required end users to authenticate with user name and password, as well as a hardware or software token, most unauthorized access could have been prevented. This is compelling intelligence.

Another addressable vulnerability exists because of a lack of controls found on outbound traffic. The 2011 DBIR shows that 92% of data breaches are external to the victim entity. In other words, criminals access a victim's facilities through wireless networking or some other external avenue of intrusion. Once they've gotten into the victim's system, cyber criminals must then find data of interest or value for the purposes of exfiltration. They must gain unauthorized access, find data and get it out without being noticed.

Most victims of external data breaches, both public and private sector, focus security countermeasures almost entirely on defending the network perimeter against unauthorized access. This is only a start. Making it difficult or impractical for criminals to exfiltrate stolen information is an equally effective way to prevent data breaches. Unfortunately, this approach is underutilized.

### ***Significant Improvement in Breach Detection is Needed***

2011 DBIR findings indicate that there is often a significant time lag between when a breach occurs, when data theft actually occurs and when the victim discovers the breach. This ranks among the most surprising intelligence offered by the studies, according to reader feedback. Consider the following points:

- Over the past seven years, the timeframe from initial point of entry to the first verifiable instance of data theft is more often measured in days (44%), weeks (5%) or months (4%), as opposed to minutes (33%) or hours (14%).
- The timeframe from initial point of entry to the point the victim entity first discovers the possibility of a data breach is, on average, just over 6 months.
- Even after 6 months, 86% of victim entities did not find evidence of data breach on their own – 46% found out about the problem via 3rd party fraud detection, 30% were notified by law enforcement and 6% were reported by customers or business partners who were also affected.

The very same part of the 2011 DBIR shows that in terms of data breach detection methods, countermeasures such as anti-virus, intrusion detection systems including intrusion prevention, and log review processes account for only negligible percentages (<1%). No one should infer, however, that these countermeasures are not effective.

On the contrary, our research suggests that security controls such as intrusion detection systems and log review processes are effective countermeasures when deployed as part of a defense-in-depth approach. However, at times, our VZIR team found deficiencies in the manner in which these systems were deployed and configured. Worse, even greater deficiencies were found in how these systems were operated by the victim entity on a day-to-day basis.

Deficiencies in logging and, of equal importance, meaningful reviews of logging, are factors contributing to the success of a cyber attack. Often, logging facilities are available but are disabled or reduced in capacity for performance or cost reasons. Failure to utilize log data showing inappropriate activity through a mechanical or manual review provides “cover” for bad acts. Notwithstanding the fact that some details of almost every data breach can be found in logs, victim entities rarely discover the problem on their own even after six months. As a result, real world data breaches play out over considerably longer timeframes than most anticipate.

### ***Closer Law Enforcement Cooperation Could Reduce Overall Numbers of Electronic Crimes***

Greater sharing of electronic crimes intelligence between private industry victims and law enforcement has enabled a dramatic improvement in investigative techniques and the ability of investigators to identify perpetrators conclusively. Such identification is critical to successful prosecution which, in turn, has a discernable impact in reducing cyber crimes thereafter.

The 2011 DBIR details the extent to which data breaches (92% of the total case population) can be conclusively tied back to known organized crime groups (58%), unaffiliated persons (40%), and other known adversaries. More often than not, such a conclusive identification of perpetrator(s) is possible. It shows that as of December 31, 2010, only 14% of data breaches revealed unknown or otherwise unidentifiable sources. This is significant; just a few years ago, that number was closer to 65% (based on Verizon-only figures).

With each month that passes, investigators become more capable of identifying data breach perpetrators. The discovery of common artifacts across distinct case investigations, including but not limited to IP address sources, malcode samples, attack sequences and underground chatter, makes it possible to not only reveal perpetrator(s) but also better set the stage for successful arrest and prosecution.

Open source efforts such as the VERIS framework allow for the sharing of cybercrimes intelligence among investigative groups having disparate jurisdictions and focus. In fact, the VERIS framework served as the information-sharing vehicle making the DBIR possible.

The greatest obstacle to cooperative information-sharing is the reluctance of cyber victims to engage law enforcement. VZIR often encounters a misperception by victim entities, however inaccurate and unfounded, that notification of law enforcement is tantamount to an open public disclosure. They avoid such notification in an attempt to sidestep fines, penalties and general dispute litigation stemming from disclosures. Further, when law enforcement authorities are already involved, this perception drives data breach victims to cooperate only in part or to the minimum extent necessary.

While notifications to consumers serve an important role to protect individuals in certain instances, a notice is most effective when it is limited to instances where the breached data elements impose an actual risk of harm, such as a social security number or financial account number. Requiring consumer notifications for data elements that do not create a risk of harm or for identifiers that do not personally identify individuals are an unnecessary exercise that does not serve any of the stakeholders. Consumers may find such notifications confusing and learn to ignore them, eventually ignoring those that they should truly pay attention to.

Reasonable protections for victims of cyber crimes from litigation and regulatory fines would encourage cooperation between those victims and law enforcement. It would improve the odds of successful criminal prosecutions. Our research supports the notion that visible prosecution tends to have a measurable impact on total numbers of electronic crimes immediately thereafter.

Perhaps the most significant development over the past several years was the unexpected drop in IT investigations demand internationally following the Al Gonzalez arrest and prosecution here in the U.S. in 2009. During the following five-month period, VZIR observed a considerable ease in customer-demand. This finding was echoed by industry partners and in public sources of data breach disclosure tabulations. Promoting full cooperation with law enforcement and improving information sharing pathways are among the most positive steps that can be taken today to diminish the electronic crimes risks and threats we collectively face.

### ***Government's Role in Promoting Cyber Security***

As the prior discussion illustrates, there is a role for government to play in helping end users better defend themselves against advancing cyber crimes. First, government can leverage its capabilities to help conduct research and development into cyber security best practices for



end user entities. Sponsorship of fundamental educational initiatives in the area of cyber and computer security -- whether it be curriculum development for K-12 students, or advanced contests for graduate students and private sector -- can all help lead to a better equipped cyber security workforce.

Similarly, the government could take to heart many of the recommendations in the DBIR and other industry studies, and use those as a model for securing its own networks and infrastructure. Using government procurement power to dictate security requirements for systems and applications deployed by the government can go a long way to funding the availability of such resources for the private sector.

In that same vein, a single, national paradigm for reporting of high risk security breach incidents to affected individuals is crucial. With over forty different state requirements on when and how to give notice, an organization's compliance resources are wasted instead of being put to use for improving cyber security. In today's increasingly mobile society, consumers should be able to rely on a uniform and risk based process to notify them of breaches that impose a true impact on their privacy and identity. As noted above, it does not help consumers to be overwhelmed with notices of every incident, but rather meaningful notices of incidents which represent a reasonable risk of identity theft in a manner that is recognizable and efficient.

It is important to realize that there is no guarantee that an entity can make against every breach. As we have discussed above, there are some reasonable measures entities can take. An important role for government is to implement laws and incentives that enable an entity to take advantage of a safe harbor when it has proactively subscribed to a set of practices or a self regulatory program. The ultimate goal for consumers and all stakeholders should be greater information sharing and cooperation with law enforcement.

It has also been suggested in several legislative proposals that the government work with small- and medium-sized businesses to facilitate technology-transfers in the area of computer and information security.

Finally, the government should implement processes to share threat and vulnerability information with end users. In its law enforcement role, government is likely to come into possession of a vast trove of data about perpetrators, exploits, means, methods—and most notably, other potential victims. Figuring out ways to quickly disseminate information to other potential (or actual) victims presents possibly one of the biggest opportunities for beneficial government involvement in securing our nation's network-dependent industry sectors.

## ***Conclusion and Recommendations***

Cyber attacks represent very real threats to our economic prosperity and our national security. While many public and private sector remediation activities have been highly advanced and effective, our data breach investigations indicate that even greater vigilance is required. The 2011 DBIR lays out several recommendations which, if implemented, would improve the cyber security posture of financial services firms specifically and of the private and public sectors more generally. Overall, it's critical for every entity to identify a set of essential controls and to ensure their implementation across the organization without exception. More advanced controls can be implemented as necessary. The overarching message behind those recommendations is to achieve *essential* first and then worry about *excellent* later.



Remediation activities can be even more effective if legislation clearly articulates public and private sector roles and responsibilities. Government's role in helping to secure cyberspace centers on setting the example by operating highly secure networks, building strong partnerships with the private sector and improving online users' cyber-preparedness.

Mr. Chairman, I again thank you for the opportunity to appear before the Committee to discuss the important topic of cyber security and the challenges of securing end user information systems and networks. I look forward to answering any questions you may have.

United States House of Representatives  
Committee on Financial Services

"TRUTH IN TESTIMONY" DISCLOSURE FORM

Clause 2(g) of rule XI of the Rules of the House of Representatives and the Rules of the Committee on Financial Services require the disclosure of the following information. A copy of this form should be attached to your written testimony.

<b>1. Name:</b>	<b>2. Organization or organizations you are representing:</b>
A. BRYAN SARTIN	Verizon
<b>3. Business Address and telephone number:</b> 	
<b>4. Have you received any Federal grants or contracts (including any subgrants and subcontracts) since October 1, 2008 related to the subject on which you have been invited to testify?</b>	<b>5. Have any of the organizations you are representing received any Federal grants or contracts (including any subgrants and subcontracts) since October 1, 2008 related to the subject on which you have been invited to testify?</b>
<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
<b>6. If you answered .yes. to either item 4 or 5, please list the source and amount of each grant or contract, and indicate whether the recipient of such grant was you or the organization(s) you are representing. You may list additional grants or contracts on additional sheets.</b>	
<b>7. Signature:</b> 	

Please attach a copy of this form to your written testimony.