

**Testimony of Bill Conner, President and CEO of Entrust**

**Before the Subcommittee on Communications and Technology  
of the Energy and Commerce Committee  
U.S. House of Representatives**

**“Cybersecurity: Threats to Communications Networks and Private-Sector Responses”**

**February 8, 2012**

I’m Bill Conner, President and CEO of Entrust, the leader in identity-based security software solutions. On behalf of Entrust, we appreciate the opportunity to testify today.

Entrust is a world leader in securing digital identities and information. As a security software company, we are in the business of protecting our customers — and by extension your constituents — with proven technology solutions that secure digital identities and information. Over 1,200 enterprises and government agencies in more than 50 countries, including the US Department of Treasury, the Department of Justice, Department of State, and numerous Department of Energy nuclear laboratories, rely on Entrust software.

Entrust provides software solutions that protect digital identities through authentication, enforce control policies through advanced content-scanning, and protect information assets through encryption. Our mission is to work with customers to put in place the technologies, policies and procedures necessary to protect digital identities and information against the most sophisticated cybercriminals — whether they originate as external or internal threats.

**Hacking for Harm**

Experts agree that cybercrime poses a greater threat to the security of nations, corporations and individuals than ever before. In recent years, cybercriminals have moved from hacking for honor — such as for bragging rights within the hacker community — to hacking for harm and profit; in short, it’s now overt criminal activity. Increasingly, the most common victims of targeted cybercrimes are those who can least afford a major financial hit such as small businesses. With the increased dependence of the Internet to conduct business, it is no surprise that cybercrimes — ranging from identity theft to financial fraud to cyber terrorism — have dramatically increased against small and large enterprises. Unlike citizens, who are protected by FDIC regulations, businesses’ cash or intellectual property is not safeguarded by law.

**Online Security — The Ongoing Effort**

At Entrust, we are working around the world with small and large enterprises, governments and law enforcement agencies to enable security software for the good guys. We do this knowing that the total cost to deploy security is dwarfed by the cost of what is at stake. Cybersecurity is

similar — a quality-control process in that it must be disciplined, measured and continually improved upon on a daily basis. The challenge I face at the helm of Entrust is to make this possible for companies and governments in a cost-effective and uncomplicated way.

Underlying our efforts is a fundamental belief that success does not mean entities lock down their data. What it should mean to you as policy makers is that they appropriately secure their data so that the benefits of online and digital activity are not impaired, while confidence in the security of the network is maintained.

In short, if you have the image in your mind that a successful cybersecurity strategy is a moat, your strategies, laws and regulations will fail. A moat does not protect from attacks from within, which constitute nearly 80 percent of all cybercrimes. Putting all your faith in a moat also fails to adapt to new threats that defeat such an impoundment and results in data being locked down, which undermines the entire benefit of the digital economy.

The good news is that I have the opportunity to work with many of my peers in coordinating strategies to enhance the positive aspects of the Internet's promise and to combat those who abuse and attack it. There are strategies out there today that work.

But we must be ever-vigilant as cybercriminals continue to outpace our gains with new tricks and technology of their own. That is why we must fight this on a national level and involve the government, enterprises and citizens.

No one is immune. Last year alone, we saw numerous high-profile attacks ranging from Northrop Grumman to Lockheed Martin even to security companies like EMC/RSA, Comodo, Symantec and VeriSign being victims of breaches. Sophisticated attacks such as these are clear evidence that organizations need greater layered security to thwart today's savvy cyber terrorists. Our industry must be proactive in developing solutions that empower organizations to quickly respond to attacks without compromising day-to-day operations. It is also apparent that, as a nation, we are not doing enough to protect our assets and personal information.

### **The Zone Defense**

Sadly, the football season is officially over. However, it seems to me that cyber defense is much like playing defense in football — you don't know what play the other team is calling, therefore, you need to defend against everyone. We first need to understand what offensive strategy we are up against. If the offense sees a hole in your front line, they will exploit it. If they see you are exposed in the secondary, they will attack there. And they will keep trying new angles until you react to shut down that vulnerability.

Cyber security is much the same way — businesses do not know how they will be attacked. They don't know if the threat comes due to a download from an employee surfing the Web, via an attack from within, or from a virus that may have entered the system on an email. What we

do know is, that to win, large government and private organizations of all sizes need to have a strategy to deal with the range of threats. If we wait until we are hacked, it's too late.

Cybercriminals will search for that open door and if they find it, they will wreak havoc on data and possibly divert a company's payments or IP to the bad guys. Consider the amount of time and money it takes a company that has lost all its data to a cyber-attack — not to mention the significant hit to the credibility they lose with their customers if a cybercriminal stole personal information.

Let's be clear. What we face is a threatening cyber environment where warfare is being conducted by foreign governments, international crime rings and common thieves in the U.S. It takes everyone — government, major organizations, small businesses and individuals — working together to defeat those forces.

### **Moore's Law**

To put this all in context, hardware technology follows Moore's Law, which states that capacity doubles and cost halves every 18 months. In the new cyber world, software tools are changing in days, not years, and in many cases hours or even minutes. That makes it a constant real-time battle for all of us.

We are facing a wide range of extremely dangerous enemies armed with expensive and sophisticated hardware, software and boldness. They function in an environment where their white-collar crime, even if identified and apprehended, brings only minimal punishment. This is because most of these attacks are across sovereign borders around the globe.

The good news is that technology and solutions exist today to thwart these cybercriminals. However, it must be applied consistently and universally to deny cybercriminals the easy access they have today.

### **Shortcomings of FFIEC Guidelines**

Let me give you a specific example. The Federal Financial Institutions Examination Council (FFIEC) recently updated its guidance for financial institutions offering Internet-based products and services. Unfortunately, these guidelines only hit at the minimum level of security and are already outdated.

Just like the guidance they released in 2005, the guidelines do not place accountability for implementation nor do they mandate any specified timeframe. This puts consumers and businesses at risk when they conduct business online with their bank. And worse yet, it gives the false impression to consumers and the marketplace that entities are safe when, in reality, they are barely doing anything at all.

Even more alarming, the updated FFIEC regulations do nothing to help small- and medium-sized businesses. So while the guidance falls short of protecting larger financial institutions, it's also all but ignoring the organizations that may need the most legal protection.

### **Diagramming Advanced Malware**

With that in mind, here is one example of a real-world threat that we have encountered that has not received as much attention as data breaches. It is, however, one of the biggest cybercrimes and threats today. The threat is called ZeuS or SpyEye, which is a "man-in-the-browser" malware that targets mid- to small-sized companies. This is a threat you and your constituents need to be aware of and concerned about.

The problem arises when someone within an organization is surfing the Web and accidentally installs software that opens a door for criminals. The software may install when an employee has visited a legitimate website, but one that has unknowingly become infected, or they may have simply clicked the red "x" to close a pop-up ad or notification thinking that all they were doing was shutting down the ad.

In reality, that click prompts the malware to install on their system and then promptly hides itself. In fact, once the malware is installed it is extremely difficult to detect. The malware is crafted to avoid detection by antivirus tools that you all know and probably use.

This malware sits dormant, waiting for someone on the system to log in to a corporate bank account online. When it sees that bank URL pass by, it wakes up and begins to intervene transparently in whatever transaction is being conducted.

Let me explain how it works.

- A consumer, or more likely an accountant, in a small business initiates an online payment to their local utility for \$1,000.
- The malware on a PC, laptop or tablet sees the bank URL and online payment. It then "wakes up" and translates that payment into, let's say, six different transactions totaling \$100,000 going to six individual accounts.
- The bank then receives the request for these six transactions totaling \$100,000 and asks the accountant to confirm the transactions by entering a one-time passcode (OTP) to authenticate the transactions.
- The malware intercepts this request and re-translates the six transactions back to the original single transaction for \$1,000.
- The accountant, therefore, sees the original request for the utility to be paid \$1,000 and is asked by the bank to enter their specific one-time passcode.

- The controller then enters a one-time passcode to authenticate the transaction and sends it back to the bank.
- Unfortunately, the malware accepts the one-time passcode and again re-translates the single \$1,000 transaction to the six transactions totaling \$100,000.
- The bank then believes it is a set of authorized corporate transactions based on the passcode the client provided and executes those transactions for \$100,000.
- Now both the small business and the bank are missing \$100,000.

This is the kind of threat that can and does happen in every state, every day. And not just at multinational companies. It can and does happen to smaller enterprises that aren't as sophisticated in how to protect themselves nor consider themselves to be a target of multinational crime schemes. But they are wrong. This has and does happen to businesses that populate Main Street in every state.

### **Malware Hitting Home**

Let me give you a real-life example. Plano, Texas-based Hilary Machinery, one of the largest machine tool distributor service organizations in the southwest, had \$800,000 drained from its bank accounts in two days. It wasn't the company's financial institution that discovered the error. It was Hilary Machinery itself.

Between November 9-10, 2009, PlainsCapital Bank received fraudulent wire-transfer instructions from a group that infiltrated the bank accounts of Hilary Machinery. Some of the transfers involved sums in excess of \$100,000, while others were as small as \$2,500. Each transfer was made to a different account, which was highly unusual, and outside the norm for the company. PlainsCapital Bank was able to recover all but approximately \$200,000 of the lost funds.

Now, who is responsible for the loss was a matter of question. Hilary Machinery believed that PlainsCapital should have been held liable, sued the bank and demanded repayment of the remaining \$200,000.

In turn, PlainsCapital counter-sued, saying their security was, in fact, reasonable by industry standards and that it processed the wire transfers in good faith. The lawsuit was eventually settled, but the point is that this could have happened to any small business in terms of the attack and fallout. Compounding the problem is that, if this theft had affected an individual, at least the FDIC would have made them whole. But small-business accounts aren't protected. So they are out the money unless they have the means to sue and the amount of loss is more than the cost of litigation.

Also, this is the silent crime. Small businesses that have been hit do not have PR shops or press agents and have little reason to let the public know they have been impacted. And the banks have little incentive to tell consumers that their fraud detection and passcode methods do not actually work against such threats. So while this cybercrime is widespread, you do not hear about it and that leaves more and more companies unaware that they need to do more.

### **SMBs at Risk**

Unfortunately, this example shows just how vulnerable small- and mid-sized businesses can be and demonstrates the potential fallout of not having a strong cyber defense. There is no clear law or legislation that protects companies or provides guidelines on what they, their vendors or their financial institution need to have in place to protect sensitive data.

It also varies from state to state, so the burden is on each company to figure it out relative to their situation and possible exposure. It often comes as a surprise to companies I speak with; small- and mid-size businesses do not have the same protections as individuals. Again, it falls on their shoulders to ensure they are protected.

And just because you are a small business doesn't mean cybercriminals aren't going to target you. In fact, according to the Federal Communications Commission, three of every four small- and mid-sized businesses report being affected by cyberattacks.

An employee may get an email that looks valid and opens it, clicking on a link. It turns out to be a phishing scheme. It's happened time and time again with an array of targets including huge companies like Google, University of Wisconsin-Milwaukee, a Dallas-based business telephone equipment company, a Missouri dental practice and even cities such as Brigantine, New Jersey.

### **Security 101**

The good news? There are inexpensive and intuitive tools to combat this kind of threat. So what are small and large enterprises, financial institutions and governments to do?

First, in my mind, are the cybersecurity basics — or table stakes, as you might call them — for online security. Employees must have at least basic training on security practices to protect sensitive business information, communication and transactions.

Organizations also need to ensure that computers and networks are protected from viruses, spyware and other malicious code. A firewall must be in place — not only at the point of connection to the Internet but on all computers, including laptops used to conduct company business. And, finally, the proper settings must be routinely checked for vulnerabilities and attacks.

Education, coupled with dedicated perimeter security solutions, provide the first basic layer of protection for businesses and its employees.

Another key to cybersecurity across an organization pertains to the downloading of software. I cite Brian Krebs's blog from May 2011 — "[Krebs's 3 Basic Rules for Online Safety](#)" — where he gave three basic rules for online safety in this area.

- First, "**If you didn't go looking for it, don't install it.**" You are taking a great risk by downloading software that you don't directly know.
- Second, "**If you installed it, update it.**" Basically, keep up with new versions of software because they include updated security for vulnerabilities that have been found in earlier versions.
- And finally, "**If you no longer need it, remove it.**" Unneeded software can slow down your machine and eventually open it to a wider array of breaches. In the end, it is all about keeping networks, computers and devices protected to help thwart the opportunity for someone to breach your infrastructure.

### **Identity-Based Security**

Finally, to truly secure your environment, you need a layered, identity-based security solution. You cannot have security and trust without knowing who or what is on both ends of a transaction.

To have that trust you must understand how digital identities are changing. Today's identities go well beyond people and how we have traditionally thought of identity. Digital identities now include kiosks, servers, routers, mobile devices, applications, ATMs and even power meters. This next generation of digital identities, including devices and application objects, will dwarf human identities in the next five years. Identity-based security brings this all together with the right level of security, enablement, risk and compliance to any transaction — regardless of identity type.

So, what do you need to know to secure identities?

You need to control physical and logical access to your facilities, computers, networks and any other devices that house important information or have access to your networks. And, increasingly, you will need to manage the "mobile" access of smartphones and tablets. Mobility has come of age and is the next wave of innovation — for good and for bad.

Of particular interest to this Subcommittee due to its jurisdiction, security may also rely on utilizing various telecommunications networks to conduct a single transaction. Verifying an online transaction by stepping outside that band is one simple example. Specifically, one option for parties conducting a transaction that is occurring over wired Internet connect is to agree to speak over a different network, perhaps by using a cell phone, to confirm the

transaction and the identity of the users. That would ensure that any connection that may have been compromised is quickly identified before a transaction is completed.

Lastly, you need to ask your financial institution how your business is protected should it become a victim of a cyber fraud. You may be surprised that current regulations leave many small businesses unprotected, as we saw with the case of Hilary Machinery. The ball is in your court.

You cannot assume business accounts are covered under the same federal protection as consumer accounts. Any business needs to ask its bank what current security measures it has in place. For the reasons I outlined earlier, the threats are constantly changing and, therefore, accounts must be protected against the latest threats. Financial institutions must invest in security platforms that provide the flexibility to implement new approaches and adapt to future challenges.

What I have outlined is a layered security approach, which is necessary to ensure that the right level of security is being applied to the access or transaction that is being requested. Identity-based security solutions, like those from Entrust, help you do just that.

### **Action Items**

With all of this in mind, and recognizing that this is not a legislative hearing on specific remedies, there are still three key points that Washington should keep in mind.

First, cyber security legislation must ensure there is proper corporate governance within an organization to ensure someone with appropriate authority is responsible for overseeing the cybersecurity program. It must require and recognize that cybersecurity is not a one-time fix, as was Y2K, but requires continued vigilance since threats continue to evolve rapidly.

Second, the Federal government needs to work more closely with the private sector to exchange critical information about the threats that each experiences. A perfect example of the problems that face the government and protecting itself came to light via the hacking of a well-known security company that resulted in the compromise of three Department of Defense contractors and potentially critical DOD intelligence. All three attacks leveraged the security information gained in the hack of the cybersecurity product company.

This kind of situation is persistent and we have been asking the appropriate agencies to work with us to deter further damaging breaches. Congress needs to direct the government's intelligence community to work more closely with cybersecurity companies and to share vital information on evolving threats, attack methods and how to defend against threats.

Third, the private sector would also benefit from an education or awareness campaign. While large enterprises have information security personnel, many small and medium businesses do not. The same cybersecurity companies mentioned above could work with the Department of

Commerce and the Small Business Administration to make this information available to these smaller enterprises via webinars, online guidance and checklists. The weakest link in a chain remains a real threat in the cyber world and helping educate smaller entities is a vitally important part of the puzzle.

Thank you again for this opportunity to testify and look forward to any questions you may have.