Target Under Fire for Data Breach

By now, most folks have heard about the Target Corporation breach which may have exposed 40 million U.S. debit and credit accounts, PIN numbers for debit accounts, and the personal data (name, address, phone and email) of another 70 million customers between Nov 27 and Dec. 15. There’s a good chance you may have been directly impacted by this breach, or know someone personally who has. What’s not clear is exactly what happened to cause this.

There is plenty of speculation ranging from malware making its way to the Point of Sale (POS) card swipe devices, to a potential insider job. Until the investigations are completed, we are left to monitor our accounts for suspicious activity.

9 Tips for Protecting Yourself After a Data Breach

In today’s environment, it has been said that it is only a matter of time before your personal information is compromised. The following tips are provided to assist you with protecting yourself in the event of a data breach:

- Review your credit card and debit card statements on a line-by-line basis. Thieves may place a small charge to check if the card is active, so report any questionable charge no matter how small.
- If you notice an unauthorized charge, ask your financial provider to cancel the card and issue a new one.
- Consider using monitoring tools. Target is offering a credit-monitoring service and there are other services such as BillGuard which monitor for suspicious charges.
- Be suspicious of correspondence claiming to be from your bank or retailer. Do not disclose additional personal information to a would-be thief who may use this opportunity to trick you into doing so.
- Scams also abound on Twitter and Facebook. Already a “phishing” tweet purporting to offer a link to check if you were a victim of the breach has surfaced. When you click the link, it asks you to re-enter your Twitter password. If you use the same password for your bank accounts, this could cause a greater financial problem for you.
- Double-check the URL of the bank or retailer links in any correspondence you receive. If it doesn’t look correct, don’t click it. Always go directly to a URL rather than click a link to ensure you know where you are going.
- Change your passwords, and use this opportunity to make them more complex.
- Shred documents. While the current breach is focused on electronic theft of data, it is still possible for someone to steal your paper data as well. Keep all of your data secure, not just your online information.
- Be aware if you start receiving strange pieces of mail. This could be a sign that your data has been compromised.
Cyber:
A general term for something that is related to the Internet or computers. Usually it is used as a prefix in combination with another term, such as cyberspace, cybersecurity, cyberterrorism, etc.

Botnets:
A large number of compromised computers that are used to create and send spam or viruses, or flood a network with messages as a denial of service attack.

Biometrics:
Determining what users have access to by utilizing physical characteristics.

---

**Tips & Tools**

This section is used to provide information about security tips or tools that you can utilize on your personal computers. **Please note, CEC does not support these tools (please don't contact the Service Desk for assistance).**

![Image](https://via.placeholder.com/150)

Is your web browser as secure as possible? Would you like to see how your browser security compares to other available browsers? The link below allows you to test your browser’s security against known weaknesses.


Want to test your identity theft savviness? Play this short ID Theft Faceoff game.


---

**Guest Article**

By Stephen Recca, M.A.  
(Former CTU Faculty)

The Cyber Domain: Five Ways to Frame the Security Policy Discussion

In August, 2010, the international pedophile ring Dreamboard was shut down, and 52 arrests made after a worldwide investigation led by the U.S. Department of Homeland Security. With about 600 members, the website is believed to have distributed some 123 terabytes of child pornography. It was the biggest prosecution by the U.S. of child pornographers.

In May, 2011, the Chinese Defense Ministry confirmed it has a unit of about 30 elite Internet specialists, officially said to be engaged in cyber-defense operations. Many worry, however, that the “Blue Army” has been used to hack into online systems of foreign governments.

In March, 2012, somewhere between 50,000 and 10 million credit card holders were put at risk of fraudulent charges when third-party processor Global Payments was hacked.

Over the last decade, technological advances have forced a sea of change upon the world with a myriad of positive implications. But for all the positives, there’s a dark side to our fast-evolving cyber world. There’s been a simultaneous emergence of cyber threats and crimes on a variety of fronts that pose a risk to individuals, businesses, and governments. It’s made the cyber realm a critical domain from the security perspective, and one that the public and private sectors must come together to address in a defensive manner.

That’s no small challenge: As fast as technology changes, so, too, do the threats.

Consider five areas where we should focus our thinking in order to get ahead of the curve on this evolving domain:

1. **Understand what the cyber domain encompasses.** Effectively mapping out the territory is critical to understanding its dimensions and making this sprawling domain more manageable from a policy perspective. That’s no easy task given its international nature, that it’s “owned” primarily in the private sector and by individuals, and that its tendrils spread to multiple facets of our lives, culture and society.

2. **Develop a glossary of common terms.** To enable more people to be part of the discussion requires that we adopt terms of reference that are as easily understood by laypeople as by technicians. The more easily people can grasp the terms of reference, the more broadly they can think about solutions to the issues at hand.

3. **Identify the threats putting the domain at risk.** We need ensure there’s an open aperture to capture the diversity of cyber threats. There’s hacking. There are viruses. There’s organized crime, and disorganized, as well. There’s cyber crime and cyber warfare. When it comes to crime, identity theft is a big issue for individuals, while data and systems security are major concerns for the private sector. Moreover, there are threats that cross public/private boundaries that need to be anticipated. Remember a plotline of the television show “24”? The bad guys plotted to breach our nuclear plant grid to gain control of the entire critical infrastructure protocol. The bad guys plotted to breach our nuclear plant grid to gain control of the entire critical infrastructure protocol.

4. **Identify needed resources and capabilities.** Are we equipped, from a technical and non-technical perspective, to deal with cyber threats? What will it take, now and in the future? How do we think about behaviors that will make for a more secure cyber environment? On one hand are system fixes, hardware and software considerations. On the other are capabilities that we need to study for our comfort and legal zones, not to mention our defensive posture. Are we equipped to conduct a preventive war in cyber space? To counter a cyber attack by an unfriendly nation? And, importantly, where and how do we balance investment in technology with investments in political, policy and regulatory capital?
5. **Develop a national policy using these planks as the platform.** Our policy on security within the cyber domain must reflect our best thinking on these sorts of issues, and factor in organizational considerations — who’s responsible for what, for example — to ensure we get and stay ahead of the curve on this fast-changing environment. Ultimately, it needs to represent the kind of common ground that the public and private sectors need to effectively manage the good and the bad of this brave new world.

### Recognition Corner

**CTU Students Win Top Honors at National Security Competition**

In mid-2013, Colorado Technical University (CTU) was awarded first place honors at the 7th Annual National Security Innovation Competition. This competition, presented by the National Homeland Defense Foundation, seeks to stimulate interest by college students in national security-related innovations and expose novel technologies to a broad audience.

The winning project was titled “A Novel Method to Detect the Zero-day Varian Malware and its Application on Mobile Devices” and was developed and presented by CTU students Kelly Hughes and Scott Melton under the advisement of Dr. Yanzhen Qu. The team developed a new technology that is designed to enhance protection of personal computers and wireless devices from virus attacks that come from malicious software (malware). For more information on this great achievement, please refer to the linked article below.