Deloitte.

Want to Avoid Being the Next Target, Home Depot or Canada Revenue Agency?

CIO Association of Canada
October 21, 2014

Glen Bruce

Cyber Attack Video – “Companies like yours”

The digital revolution has brought huge benefits in innovation and growth. But the heavy reliance of many business models on the Internet brings exposure to new threats. Assets that were once physically protected are now available online; customer channels are vulnerable to disruption; criminals have entirely new opportunities for theft and fraud. The barriers to cyber crime are low, the methods increasingly sophisticated and the risks of detection and capture are seen as small.

http://www.deloitte.com/view/en_GB/uk/services/audit/enterprise-risk-services/aaeeeb6f047b3310VgnVCM2000001b56f00aRCRD.htm

Headlines from the Last 7 Days

1. ***Kmart Warns Customers after Malware Discovered***
   – Sears Holding Co. reported late on Friday (Oct 10) that point-of-sale registers at its Kmart stores were compromised by malicious software used to steal customer credit and debit card information.
2. ***Phone evidence remotely wiped in police stations***
   – Tablet and smartphone remote wipe functions have been used by criminals to wipe mobile devices that were seized by officers and secured in police stations.
3. ***TD Bank Agrees to Breach Settlement***
   – Nine states impose fine after the loss of two backup tapes affecting 260,000.
4. ***SSL broken, again, in POODLE attack***
   – POODLE, allows a man-in-the-middle eavesdropper to extract session cookies from SSL sessions by forcing the victim's browser into making many thousands of similar requests, giving up clues about the encrypted secrets in the process – but difficult to actually do.
5. ***Microsoft, Adobe Push Critical Security Fixes***
   – Adobe, Microsoft and Oracle each released updates today to plug critical security holes in their products. Adobe released patches for its Flash Player and Adobe AIR software, Oracle for 25 flaws in Java and Microsoft for 24 vulnerabilities in several components.
6. ***Spike in Malware Attacks on Aging ATMs***
   – Media outlets in Malaysia reported that organized crime gangs had stolen the equivalent of about USD $1 million with the help of malware they'd installed on at least 18 ATMs across the country.
7. ***Staples Launches Breach Investigation***
   – Staples has confirmed that it's investigating a potential data breach after a report warned that elevated levels of payment card fraud had recently been tied to card numbers used by consumers who shopped at the office supply retailer.

Security Breaches remain at the top of the list of key concerns facing Canadian organizations.

Prominent Security Breaches and Themes of the Past Year

Target: Breach Caused by Malware

Retailer Confirms Attack Infected POS System

Target Corp. has confirmed that a payments breach that likely exposed some 40 million U.S. debit and credit accounts was caused by a malware attack that infected its point-of-sale system

Teen Charged in Heartbleed Breach

Allegedly Stole Data from Canada Revenue Agency

The Royal Canadian Mounted Police have arrested a 19-year-old London, Ontario, man for his alleged role in exploiting the Heartbleed vulnerability to steal data from the Canada Revenue Agency website.

Home Depot Breach Linked to Target's?

Experts Say BlackPOS Malware Is Likely Common Thread

Now that Home Depot has confirmed its payment data systems were breached, industry experts weigh the possibility that the same point-of-sale malware may have hit the home-improvement giant as well as Target Corp., Sally Beauty, P.F. Chang's and other recently breached retailers

Dairy Queen Confirms Card Breach

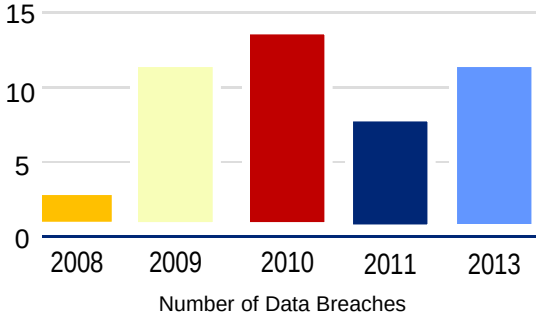
395 Locations Affected by Backoff Malware

Dairy Queen has confirmed that Backoff point-of-sale malware was used in a payment card breach that affected 395 of its 4,500 franchised U.S. locations. The ice cream and fast food chain says more than half a million

1. Information security protection is facing new challenges in dealing with **new business models** (i.e., mobile, cloud)
2. Organizations must embrace uncertainty and develop **risk resilience** not just information protection
3. Cyber security is more than managing data protection risks, it also includes **infrastructure and reputation risks**
4. The threats have become **bigger and more costly** to recover from incidents
5. bbb

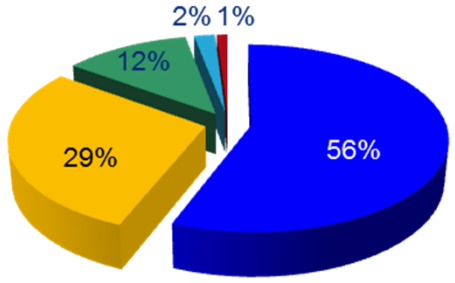
Canadian Data Breaches

How many security breaches do you estimate your organization has experienced in the past 12 months?



Source: 2014 Telus-Rotman IT Security Study

Compromised Records



Source: 2014 April-June 2014 Breach Index , Safenet

Cost of Data Breaches

The average organizational cost of a data breach:

US$ 5.85 million

The average cost per compromised record per breach:

US$ 201

Source: 2014 U.S. Cost of a Data Breach Study, Ponemon Institute

Data Breach Ranking

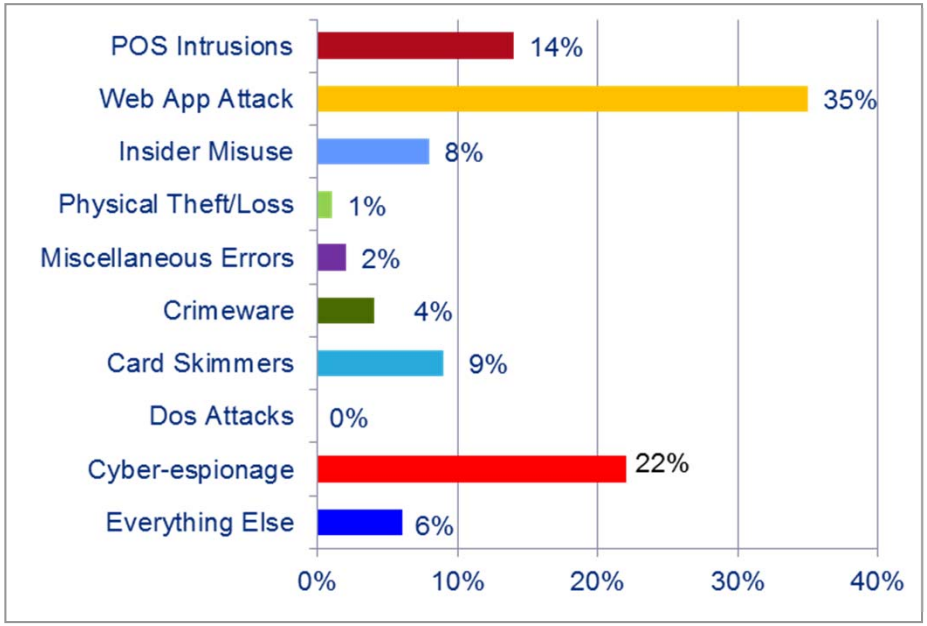
- 68% - Viruses/worms/spyware/malware/spam
- 42% - Laptop or mobile hardware device theft
- 37% - Phishing/pharming (where your organization was fraudulently described as the sender)
- 25% - Unauthorized access to information by employees
- 21% - Targeted/sophisticated attacks
- 20% - Bots (zombies) within the organization
- 18% - Abuse of wireless networks
- 15% - Denial of service attacks

Source: 2014Telus-Rotman IT Security Survey

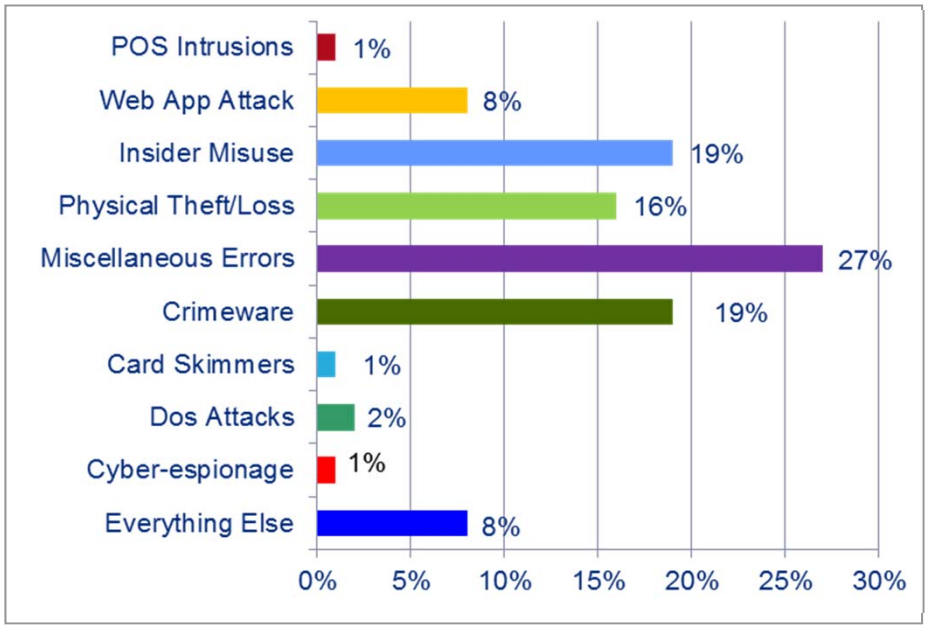
The types of security breaches have changed significantly over the years.

92% of the incidents over the past 10 years fall into 9 patterns

2013 Breaches



2004-2013 Breaches



Source: Verizon 2014 Data Breach Investigations Report,

- 2013 breach information is based on 1,367 confirmed data breaches and 63,437 security incidents
- 85% of POS breaches took weeks to discover
  - 13% took months
- 78% of incidents were discovered by an external party
  - 30% were discovered by customers
- 22% of all attacks were perpetrated by state-affiliated actors
  - 67% of state-sponsored attacks involved phishing, 20% involved Web drive-by .

Software flaws are causing major support problems

Heartbleed bug
April 2014

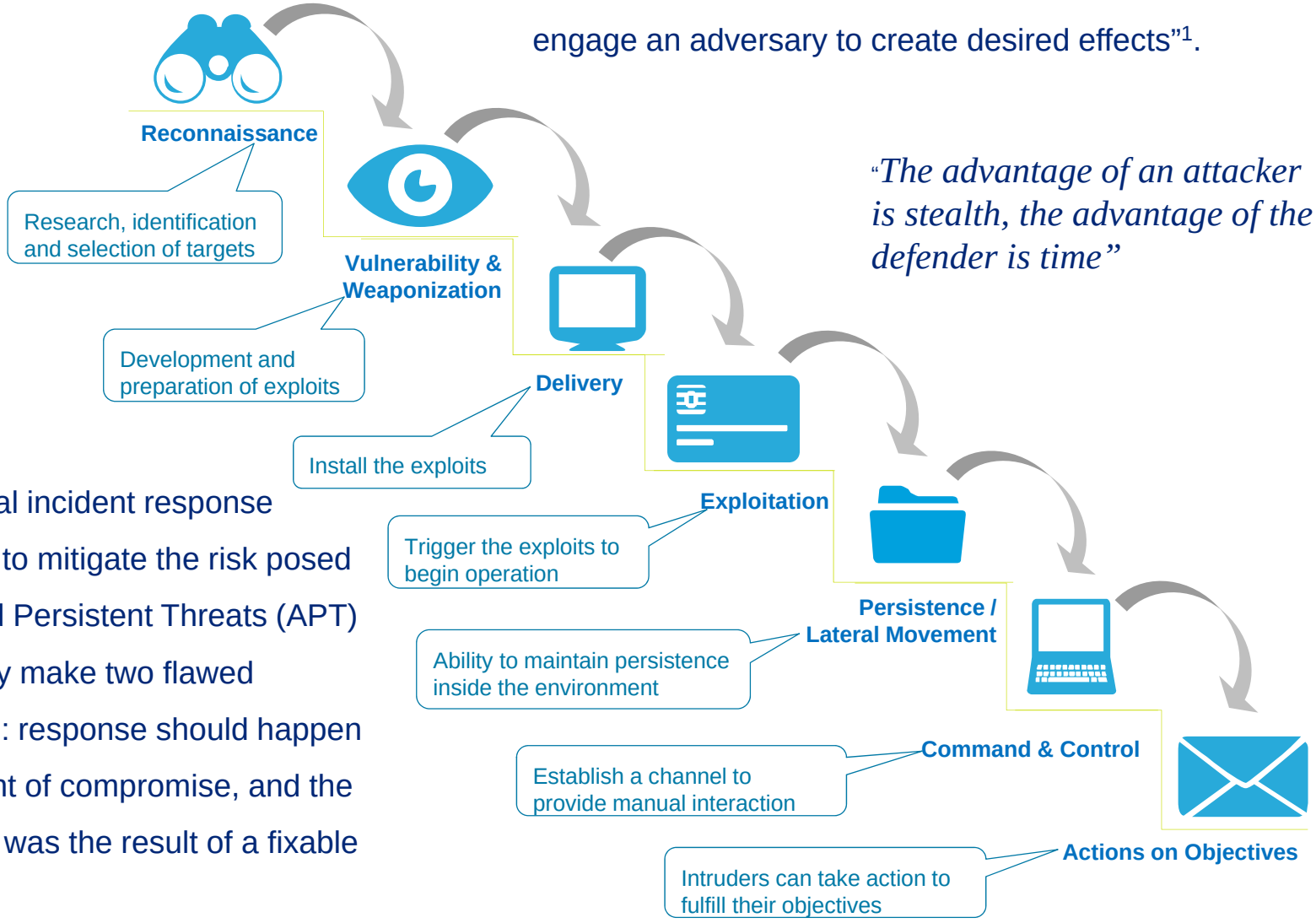
- Flaw in the OpenSSL implementation of the TLS/DTLS protocol with the “Heartbeat” function. A malformed Heartbeat request could cause the server to send back what ever is in memory – could be user IDs, passwords or other confidential information
- The flaw was present since the Heartbeat function was added to OpenSSL software in 2011. OpenSSL is used in many web servers as well as many network devices.
- The Canada Revenue Agency (CRA) was the most visible organization impacted. They took their online Tax submission facility down since the flaw could be exploited to return sensitive Tax information.
- Few major issues have been attributed to an exploit of this flaw

“Shellschock”
BASH Bug
October 2014

- GNU Borne Again Shell (BASH) is a utility that is used to translate text-based commands into command-line interfaces
- BASH is used as the default shell by many operating systems (Unix, Linux, OS X but not Windows) and is installed on millions of systems and embedded on devices
- This utility has a flaw that can allow an attacker to take complete control of a system without using a user ID and password
- Patches have been released but some of the patches have not fully fixed the problem

Cyber Kill Chain

"A Kill Chain is a systematic process to target and engage an adversary to create desired effects"[1].



"The advantage of an attacker is stealth, the advantage of the defender is time"

"Conventional incident response methods fail to mitigate the risk posed by Advanced Persistent Threats (APT) because they make two flawed assumptions: response should happen after the point of compromise, and the compromise was the result of a fixable flaw"[1].

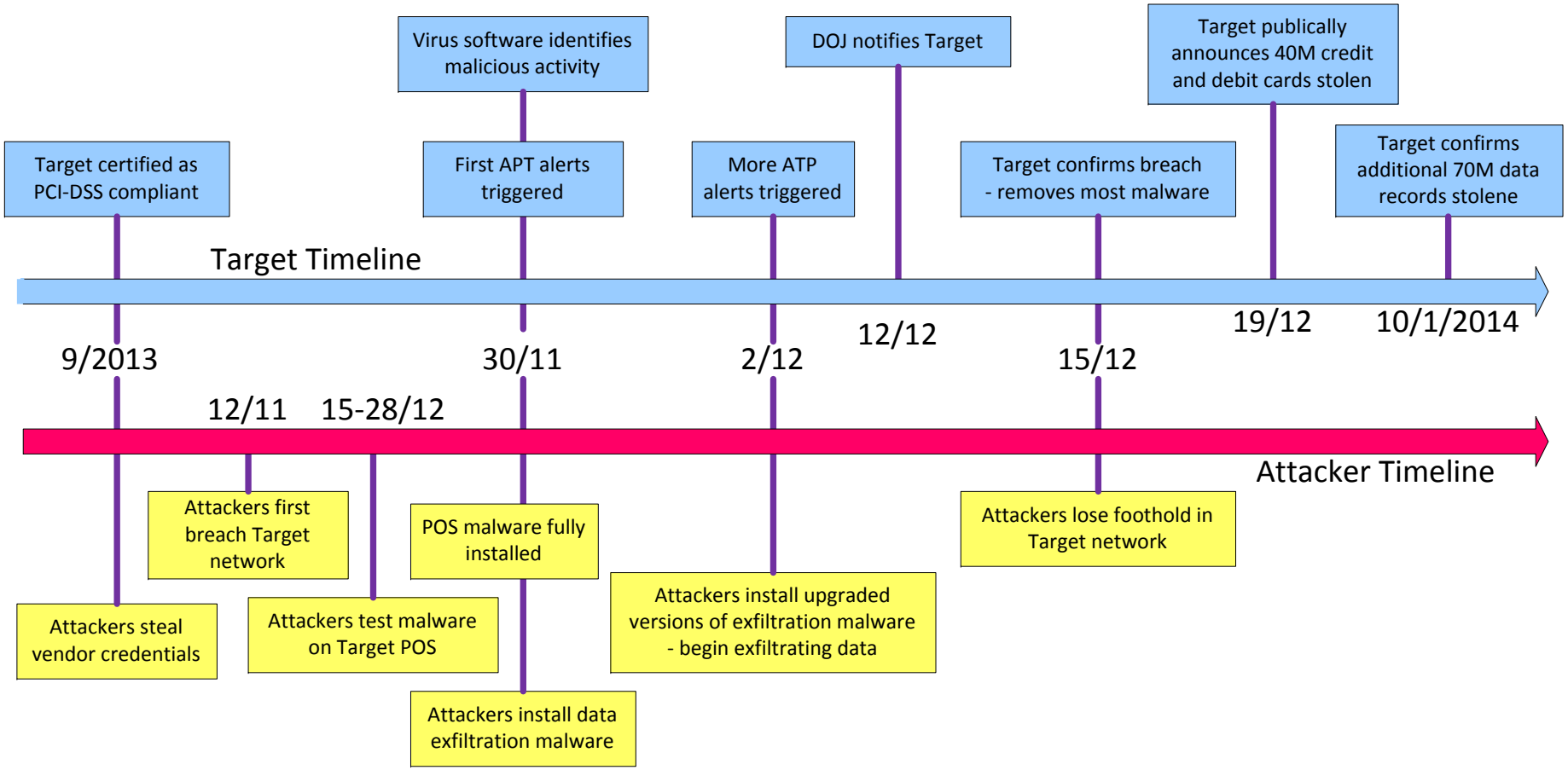
[1]Eric Hutchins, Michael Loppert, Rohan Am, Lockheed Martin Corporation.

Target Breach – Loss of 40 Million Cards

Target Breach December 2013

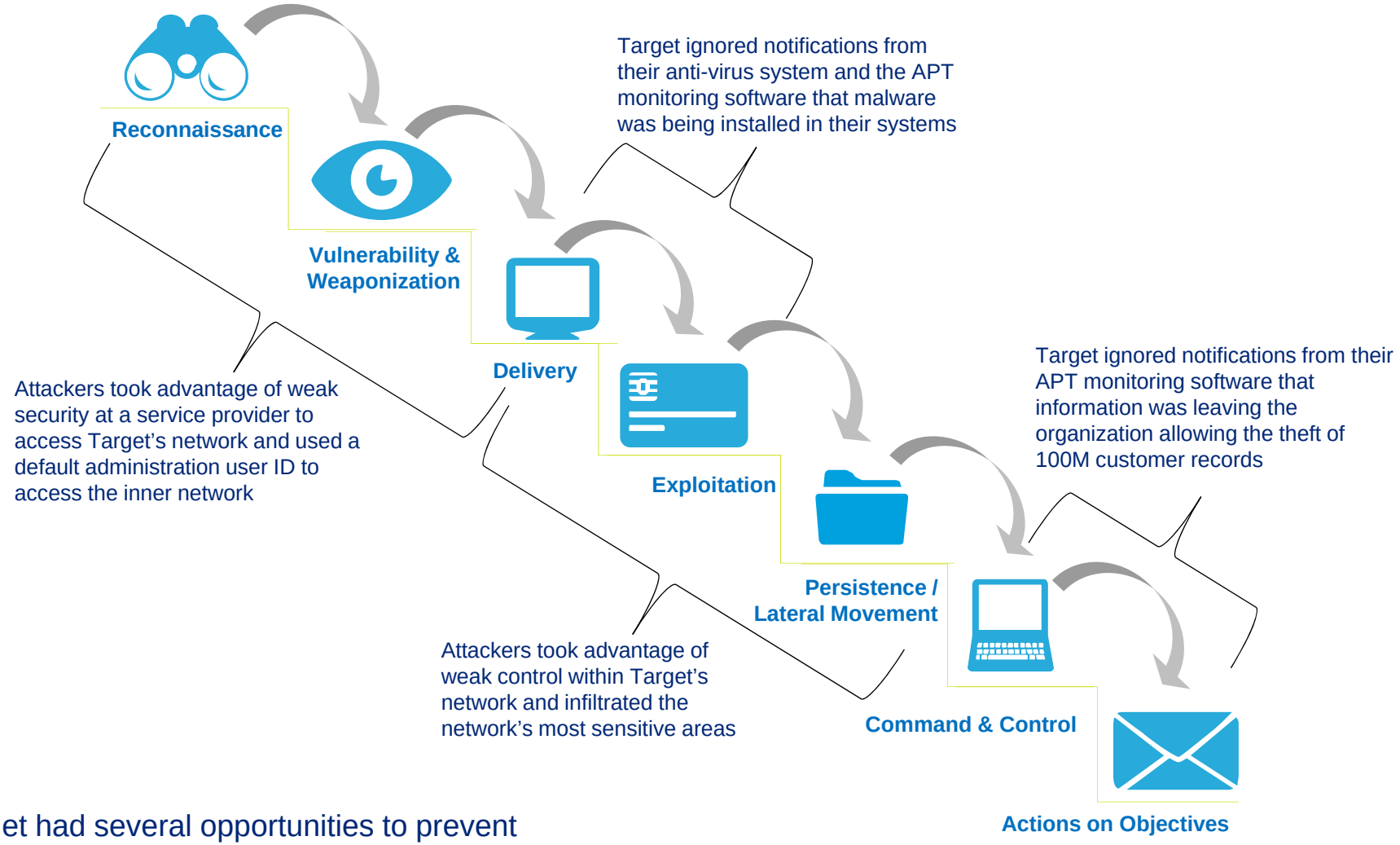
- Notified on Dec 12, 2013 by the US Dept of Justice that they had been breached
- First noticed by financial institutions indicating unusual card usage activity – all cards had recently been used at Target
- Followed by journalist who confirmed on Dec 18th that cards used at Target were for sale on a site known to sell stolen cards
- The attack actually began in September 2013 with the phishing of the credentials for a Target HVAC Service provider. These credentials were used to access the Target "outer systems"
- Access to the internal system was facilitated by using a default User ID from management software and guessing/obtaining a password
- Malware was installed that copied card data from POS devices (BlackPOS variant). Windows XP/embedded SP3 was used for the POS devices (Win XP/e is supported until 2016)
- Arranged for consolidation of card dump information on internal staging drives and then sent the copied card data to an external source.
- Anti-virus and APT detection software flagged unusual activity but the notices were not acted on.
- The malware was removed on Dec 15th

Timeline of a Data Breach - Target 40 Million Cards



- First access through a compromised business partner (phishing attack of an HVAC service provider)
- Elevated access to internal network through suspected compromise using an administration account associated with management software (default User ID *Best1_user* and password *BackupU$r*)
- Multiple failures in response to detected threats (alerts ignored)

Target intrusion kill chain missed opportunities



Target had several opportunities to prevent the intrusion from being successful.

Home Depot Breach – Loss of 56 Million Cards

Home Depot Breach September 2014

- Notified on Sept 2, 2014 by law enforcement and financial institutions that something was wrong – cards were for sale
- Breach actually began in April 2014
- Malware discovered was similar to the Target Breach – POS device memory copy of card data (BlackPOS variant)
- Breach seems to be limited to the POS devices in the self check out lanes
- Windows XP/embedded SP3 was used for the POS devices (Win XP/e is supported until 2016)
- Technology was acquired in January 2014 to encrypt the card data but was not yet installed. It has now been installed in the US but not yet in Canada
- Senior IT Security Architect was sentenced in April 2014 to serve a 4 year jail sentence from a conviction of techno-sabotage from his previous employer
- Anti-virus technology was installed in 2007 and has not been updated. It is unclear if the signatures have been maintained.
- Canadian cards do not appear to have been compromised to any great extent – likely due to the use of chip and PIN

Even more recent cyber incidents

Kmart breach October 2014

- A breach started in early September infecting the company's payment card systems – detected by Kmart's team on Oct 9th
- The breach involved debit and credit card numbers but no personal data, PINs or other customer information
- Malware was undetected by the anti-virus systems
- The number of compromised cards has not yet been released

Dairy Queen October 2014

- Dairy Queen stores breached by "Backoff" malware, payment card data stolen
- The malware impacted 395 of the companies 4,500 stores starting from August 1st to October 6th, 2014
- Dairy Queen was informed by law officials about the breach – they had not detected it.
- The POS systems in all 395 stores impacted by the malware were by a compromise of the account credentials of the same 3rd party service provider.

Lesson learned for managing cyber security risk

- Significant breaches rarely involve a **single** weakness or vulnerability
- A determined attacker will discover **all** of your weaknesses and tailor an attack accordingly
- Effective security must include the **entire** organization as well as **all** service providers and business partners
- Be able to detect suspicious activity and be the **first** to know you have been compromised
- Pay attention to your security tools and **always** follow up suspicious activity
- Ensure your protections and tools are **all** up to date and supported
- Regularly assess **all** elements of the security system and act on all weaknesses
- Plan for attacks and take **immediate** action when one is recognized or suspected

- Do you know…
  - What is **leaving your network** and where is it going?
  - Who is really **logging into your network** and from where?
  - What information are you **making available** to a cyber adversary?
  - Who is **supporting** your security and managing your risk?

For more information

If you would like more information on emerging security trends, strategies and best practices, or how Deloitte can help your organization, please contact one of the following professionals:

Tejinder Basi
Partner
Enterprise Risk
604-640-3255
tbasi@deloitte.ca

Tarlok Birdi
Senior Manager
Enterprise Risk
604-640-3148
tbirdi@deloitte.ca

Glen Bruce
Director
Enterprise Risk
604-640-3143
glebruce@deloitte.ca


Deloitte.