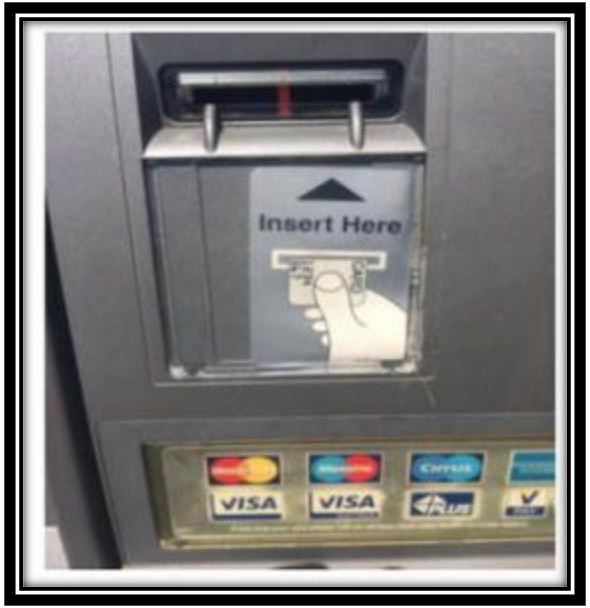
NRF®

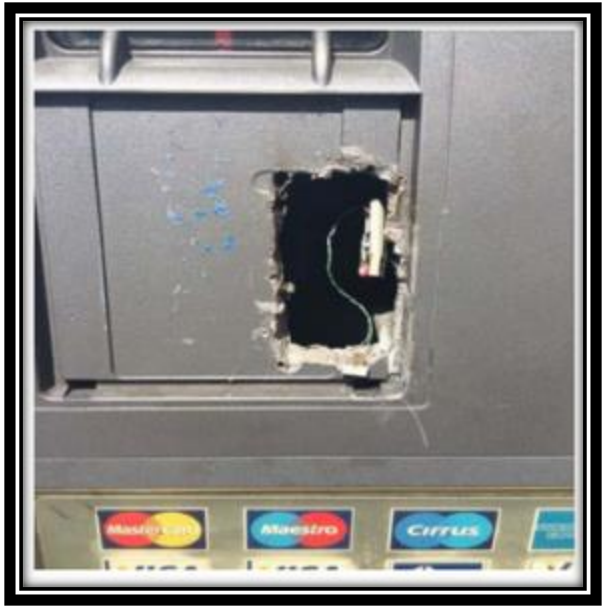
NATIONAL RETAIL FEDERATION®

RETHINKING ORC: NRF'S CYBER SECURITY EFFORTS

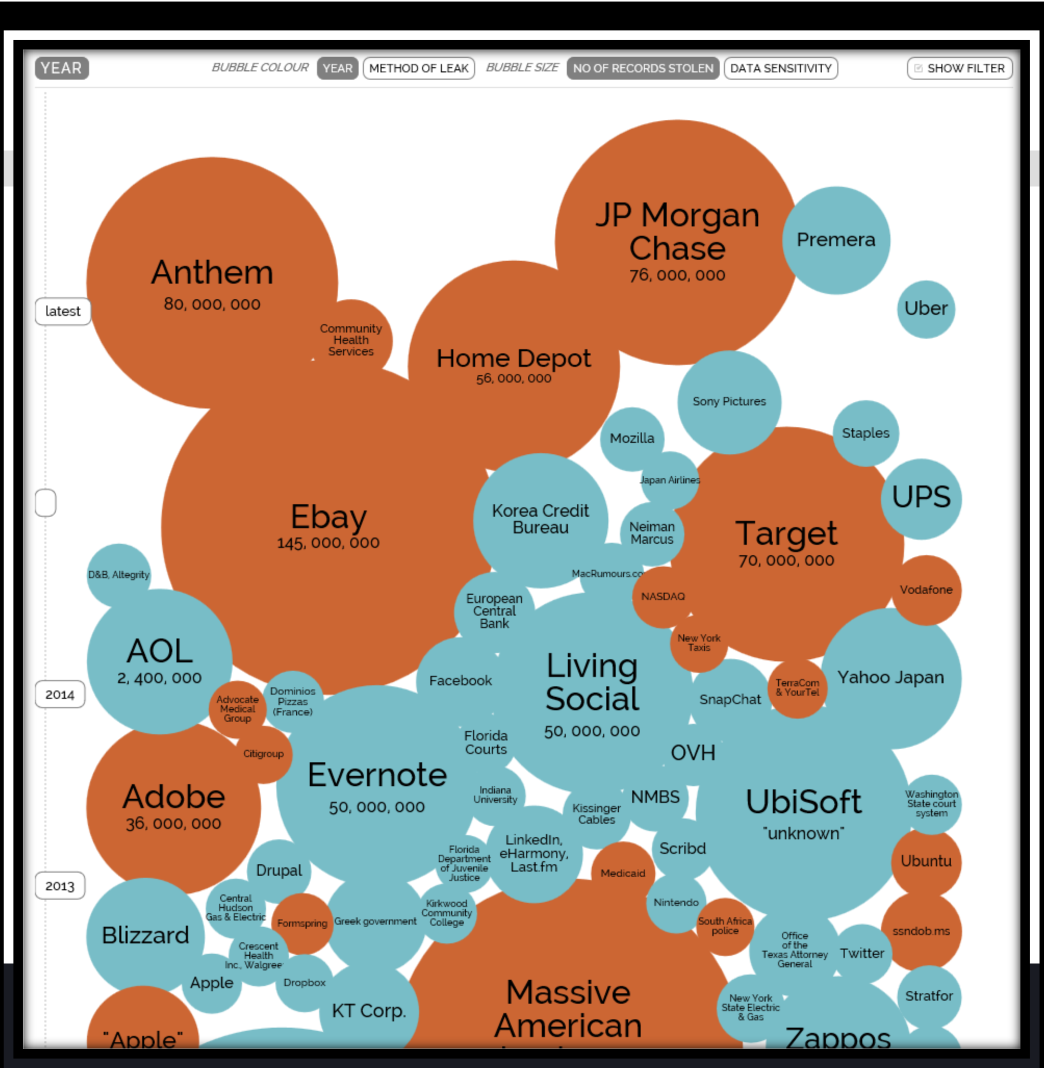
OMG Cross Domain Threat & Risk

Information Exchange Day, March 23, 2015


Insert Here
VISA
VISA


MasterCard
Maestro
Cirrus

No Organization is Secure



Source: http://www.informationisbeautiful.net

An Average Day in an Enterprise Organization

Every **1 min** a host accesses a malicious website

Every **3 mins** a malicious bot is communicating with its command and control center

Every **9 mins** a High Risk application is being used

Every **10 mins** a known malware is being downloaded

Every **27 mins** an unkown malware is being downloaded

Every **49 mins** sensitive data is sent outside the organization

Every **24 h** a host is infected with a malicious bot

Source: Check Point Security Report 2014

The Retail Industry is a Lucrative Target

Volume of investigations increased **54 percent** in 2013, compared to 2012

45 percent of data thefts involved non-payment card data

E-commerce made up **54 percent** of assets targeted – **up 5 percent YOY**

Point-of-sale (POS) breaches accounted for **33 percent** of all investigations

US retailers accounted for **59 percent** of the victims – **4x any other country**

71 percent of compromise victims did not detect breaches themselves

Source: 2014 Trustwave Global Security Report

Cybercrime: By the Numbers…

40M, 70M – number of credit and debit cards stolen from Target between Nov. 27 and Dec. 15, 2013, and the number of records stolen that included PII data of Target customers

46%, $148M – the percentage drop in profits at Target in 4Q2013 YOY, and the estimated cost to Target for their fiscal 2Q2014 responding to the data theft

$100M, 0 – the number Target says it will spend upgrading to EMV (Chip & PIN), and **ZERO**: the number of customer cards that EMV would have been able to stop the bad actors from stealing from Target

$2,500-$6,500 – the estimated cost to hackers for POS malware advertised in online freelance IT marketplaces

$18.00-$35.70, 1-3M, $53.7M – the median price range per card stolen and resold on the black market, and the number of stolen Target customer cards successfully sold on the black market and used for fraud, and the income that hackers likely generated

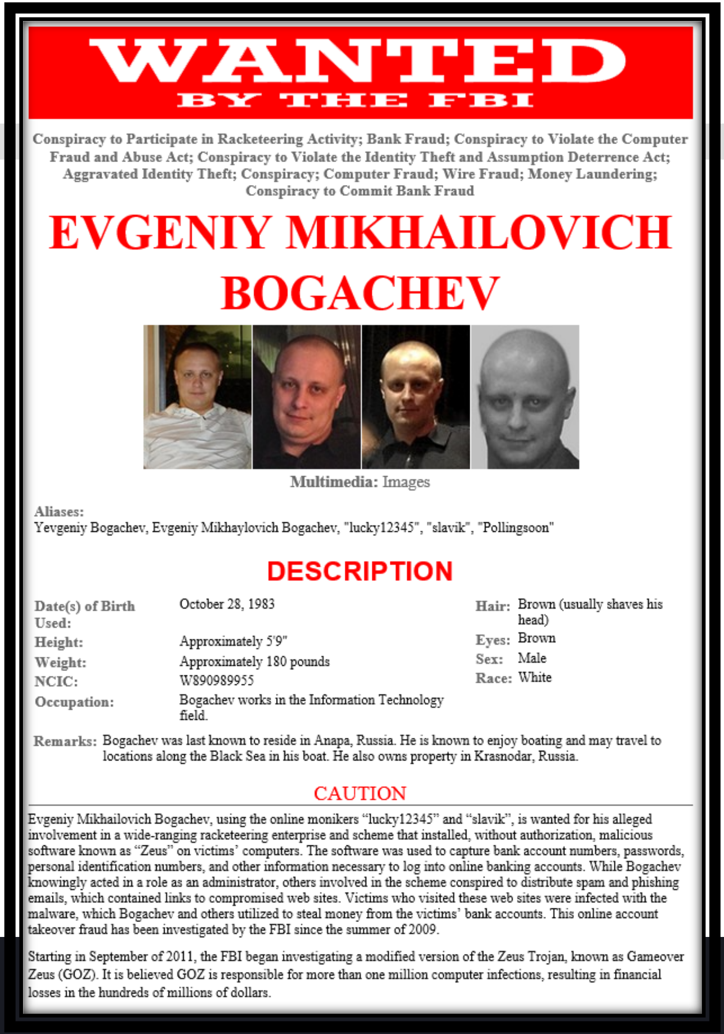
$198,234.93

haysite

haysite
reinforced plastics

Gameover Zeus

CryptoLocker



WANTED
BY THE FBI

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

EVGENIY MIKHAILOVICH BOGACHEV

Multimedia: Images

Aliases:
Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

DESCRIPTION

Date(s) of Birth Used:	October 28, 1983	**Hair:**	Brown (usually shaves his head)
Height:	Approximately 5'9"	**Eyes:**	Brown
Weight:	Approximately 180 pounds	**Sex:**	Male
NCIC:	W890989955	**Race:**	White
Occupation:	Bogachev works in the Information Technology field.		

Remarks: Bogachev was last known to reside in Anapa, Russia. He is known to enjoy boating and may travel to locations along the Black Sea in his boat. He also owns property in Krasnodar, Russia.

CAUTION

Evgeniy Mikhailovich Bogachev, using the online monikers "lucky12345" and "slavik", is wanted for his alleged involvement in a wide-ranging racketeering enterprise and scheme that installed, without authorization, malicious software known as "Zeus" on victims' computers. The software was used to capture bank account numbers, passwords, personal identification numbers, and other information necessary to log into online banking accounts. While Bogachev knowingly acted in a role as an administrator, others involved in the scheme conspired to distribute spam and phishing emails, which contained links to compromised web sites. Victims who visited these web sites were infected with the malware, which Bogachev and others utilized to steal money from the victims' bank accounts. This online account takeover fraud has been investigated by the FBI since the summer of 2009.

Starting in September of 2011, the FBI began investigating a modified version of the Zeus Trojan, known as Gameover Zeus (GOZ). It is believed GOZ is responsible for more than one million computer infections, resulting in financial losses in the hundreds of millions of dollars.

NRF's Technology Leadership Community

NRF® CIO COUNCIL

CIO Council

- An invitation only committee made up of retailing's most prominent chief information officers.

NRF® IT SECURITY COUNCIL

IT Security Council

- An invitation only committee made up of retailing's leading technology security experts.

ARTS® NRF's RETAIL TECHNOLOGY STANDARDS DIVISION

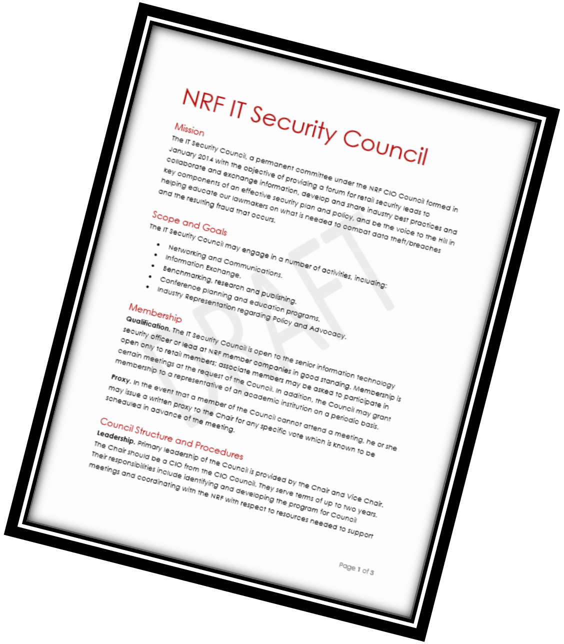
Association for Retail Technology Standards (ARTS)

- A worldwide community of retail business and information technology professionals organized to help retail enterprises and solution providers identify, adopt and integrate current and emerging technologies into their organizations, strategies and operations.

NRF's IT Security Council

Providing a forum for networking and collaboration and exchange of information, develop and share industry best practices and key components of an effective security and risk management framework, and be the voice to the Hill in educating lawmakers on what is needed to combat data theft and the resulting fraud that occurs.

- □ Networking and communications
- □ Real-time information exchange
- □ Benchmarking, research and publishing
- □ Conference planning and education programs
- □ Industry representation regarding Policy and Advocacy



NRF IT Security Council

Mission

The IT Security Council, a permanent committee under the NRF CIO Council formed in January 2014 with the objective of providing a forum for retail security leads to collaborate and exchange information, develop and share industry best practices and key components of an effective security plan and policy, and be the voice to the Hill in helping educate our lawmakers on what is needed to combat data theft/breaches and the resulting fraud that occurs.

Scope and Goals

The IT Security Council may engage in a number of activities, including:

- Networking and Communications.
- Information Exchange.
- Benchmarking, research and publishing.
- Conference planning and education programs.
- Industry Representation regarding Policy and Advocacy.

Membership

Qualification. The IT Security Council is open to the senior information technology security officer or lead at NRF member companies in good standing. Membership is open only to retail members; associate members may be asked to participate in certain meetings at the request of the Council. In addition, the Council may grant membership to a representative of an academic institution on a periodic basis.

Proxy. In the event that a member of the Council cannot attend a meeting, he or she may issue a written proxy to the Chair for any specific vote which is known to be scheduled in advance of the meeting.

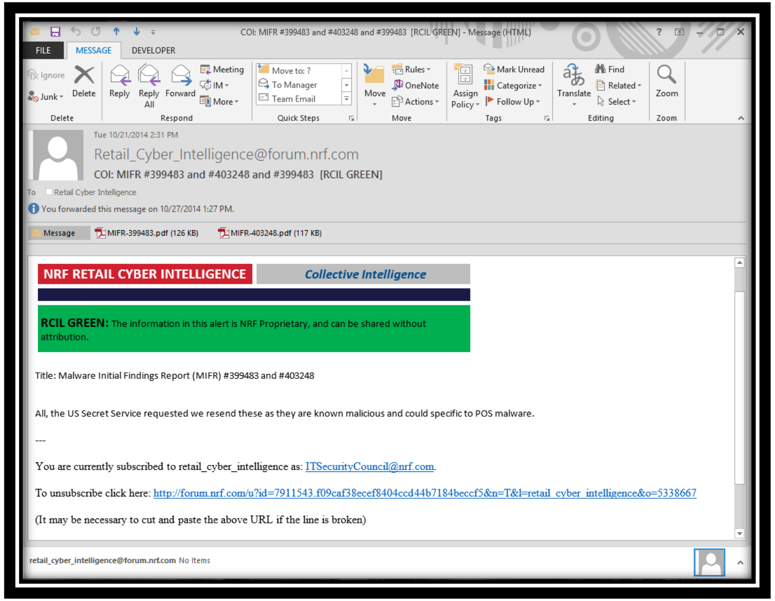
Council Structure and Procedures

Leadership. Primary leadership of the Council is provided by the Chair and Vice Chair. The Chair should be a CIO from the CIO Council. They serve terms of up to two years. Their responsibilities include identifying and developing the program for Council meetings and coordinating with the NRF with respect to resources needed to support

Page 1 of 3

NRF Threat Alert System

Facilitating Real-Time Information Exchange



Tue 10/21/2014 2:31 PM

Retail_Cyber_Intelligence@forum.nrf.com

COI: MIFR #399483 and #403248 and #399483 [RCIL GREEN]

To □ Retail Cyber Intelligence

You forwarded this message on 10/27/2014 1:27 PM.

NRF RETAIL CYBER INTELLIGENCE *Collective Intelligence*

RCIL GREEN: The information in this alert is NRF Proprietary, and can be shared without attribution.

Title: Malware Initial Findings Report (MIFR) #399483 and #403248

All, the US Secret Service requested we resend these as they are known malicious and could specific to POS malware.

You are currently subscribed to retail_cyber_intelligence as: ITSecurityCouncil@nrf.com.

To unsubscribe click here: http://forum.nrf.com/u?id=7911543.f09caf38ecef8404ccd44b7184beccf5&n=T&l=retail_cyber_intelligence&o=5338667

(It may be necessary to cut and paste the above URL if the line is broken)

retail_cyber_intelligence@forum.nrf.com No Items

- □ Partnering with FS-ISAC, US government (NCCIC, US CERT, US Secret Service), and private sector intelligence providers
- □ Averages 12-15 structured alerts per day
- □ Coded by Incidents, Threats, Vulnerabilities and Resolutions
- □ TLP Protocol enforced
- □ Separate collaboration portal

Deloitte.

NRF NATIONAL RETAIL FEDERATION

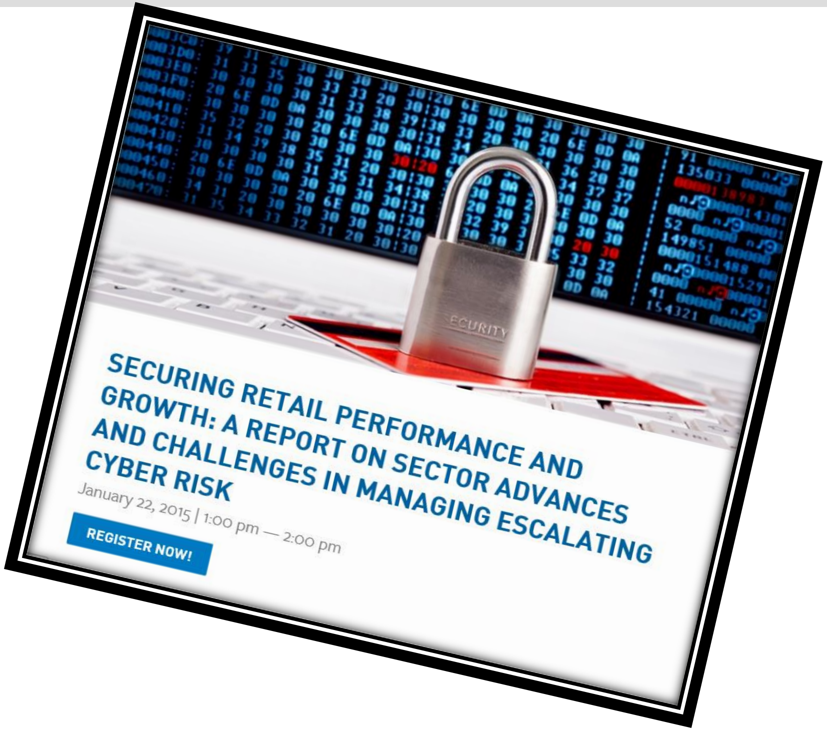
Retail Cyber Risk Leadership Forum

Protecting the business to secure tomorrow's growth

IT Security Webinar Series

Education

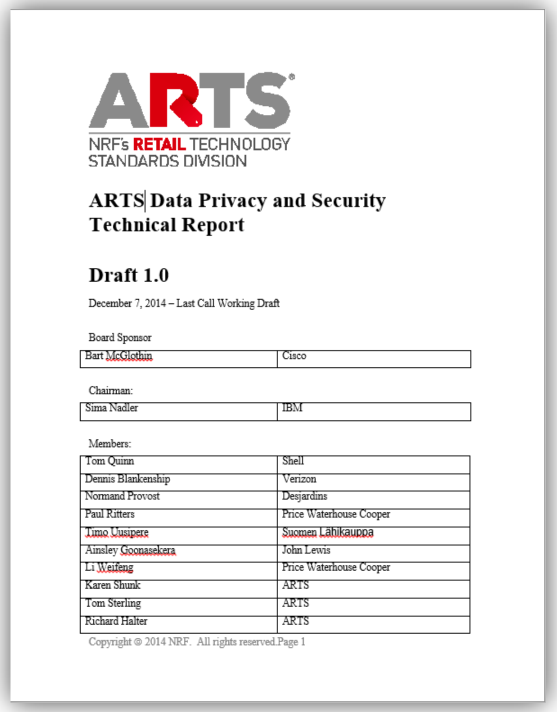
- □ Target POS Malware Debrief
- □ P2P Encryption & Tokenization: Ready for Primetime!
- □ Planning a Secure Payments Strategy
- □ Switching Gears: PCI DSS 3.0
- □ Merchant Considerations for US Chip Migration
- □ Securing Retail Performance and Growth



SECURING RETAIL PERFORMANCE AND GROWTH: A REPORT ON SECTOR ADVANCES AND CHALLENGES IN MANAGING ESCALATING CYBER RISK

January 22, 2015 | 1:00 pm — 2:00 pm

Benchmarking, Research & Publications



ARTS®

NRF's RETAIL TECHNOLOGY STANDARDS DIVISION

ARTS Data Privacy and Security Technical Report

Draft 1.0

December 7, 2014 – Last Call Working Draft

Board Sponsor

Bart McGlothin	Cisco

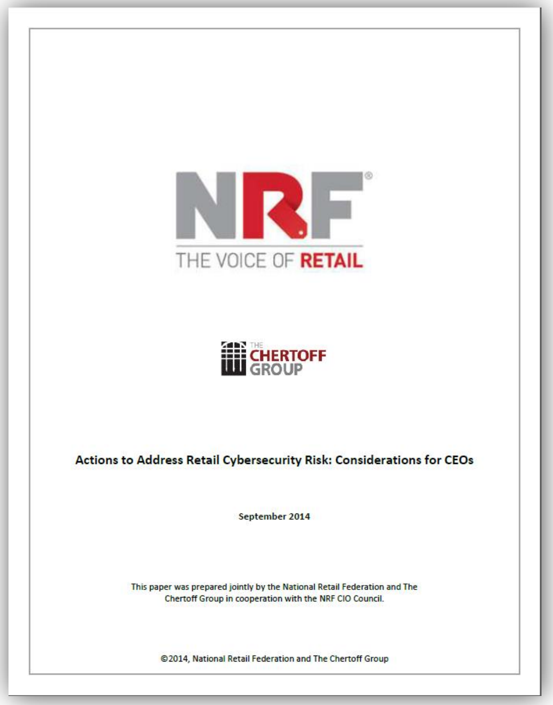
Chairman:

Sima Nadler	IBM

Members:

Tom Quinn	Shell
Dennis Blankenship	Verizon
Normand Provost	Desjardins
Paul Ritters	Price Waterhouse Cooper
Timo Uusipere	Suomen Lahikauppa
Ainsley Goonasekera	John Lewis
Li Weifeng	Price Waterhouse Cooper
Karen Shunk	ARTS
Tom Sterling	ARTS
Richard Halter	ARTS

Copyright © 2014 NRF. All rights reserved Page 1



NRF®

THE VOICE OF RETAIL

THE CHERTOFF GROUP

Actions to Address Retail Cybersecurity Risk: Considerations for CEOs

September 2014

This paper was prepared jointly by the National Retail Federation and The Chertoff Group in cooperation with the NRF CIO Council.

©2014, National Retail Federation and The Chertoff Group

Deloitte.

NRF® NATIONAL RETAIL FEDERATION®

Securing Retail Performance and Growth

A report on sector advances and challenges in managing escalating cyber risk

Coming Soon!

DRAFT
DO NOT DISTRIBUTE

"Stay left of boom"

1. Act like a CSI…
2. Build the muscle of a first line of defense…
3. Have an actionable Incident Response Plan…
4. Watch your supply chain…
5. Think of all your threat vectors…
6. Wall off your most critical data…
7. Share your intelligence…
8. Become the hunter…

"Your adversary has to be right 100% of the chain [of events]. You only have to break it in one place."

Source: Sondra Barbour, EVP, Lockheed Martin, notes from the Gartner Symposium, October 2014

Understanding Cyber Risk Management

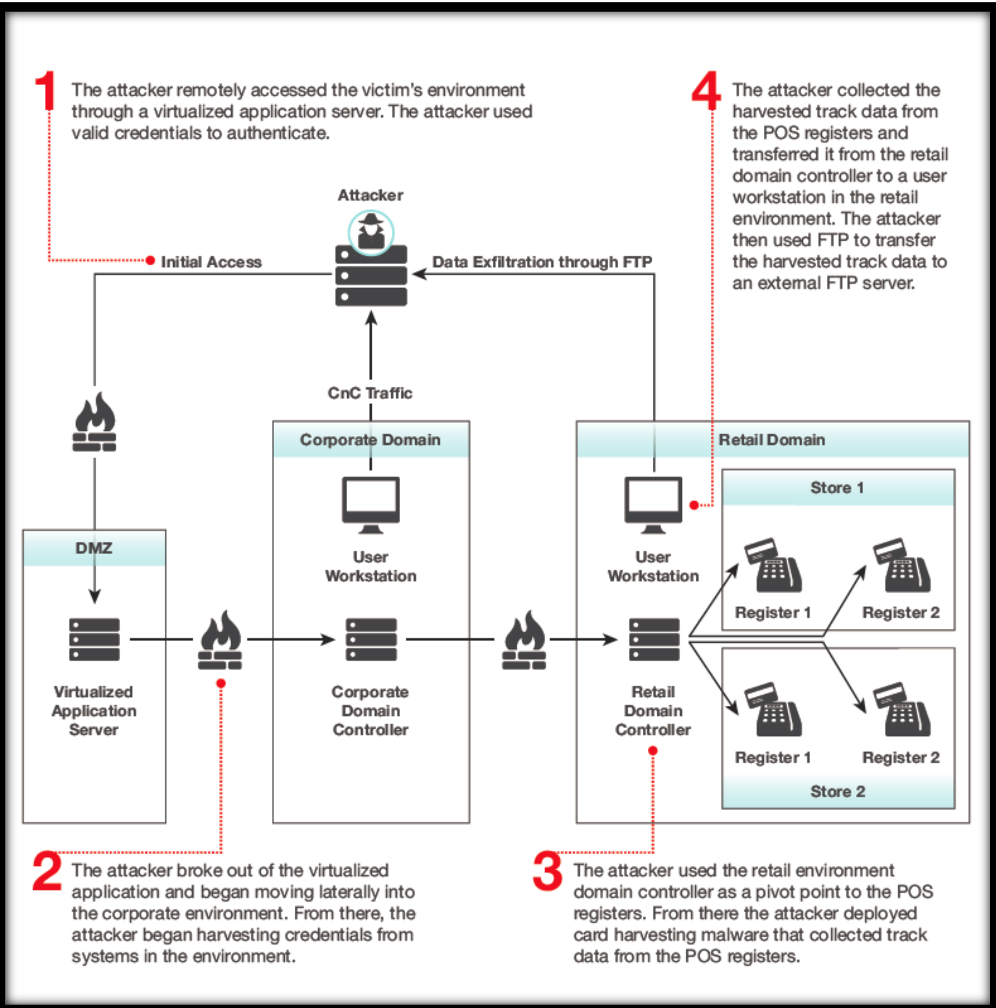
1. How is our executive leadership informed about the current level of cyber risks to our company? How is security reflected in our culture?
2. What individuals within the company are responsible for aspects of cybersecurity, including network security, physical security, breach response, and risk mapping? Do we have a formally designated, qualified Chief Information Security Officer or equivalent?
3. How does our cybersecurity program apply industry standards and best practices, including the NIST Cybersecurity Framework?
4. How have we prioritized cybersecurity risks, and what is our plan to address identified risks? Do we consider cybersecurity risks up-front in new business initiatives and new technology implementations?
5. How do we manage risk related to vendor access to our systems and information?
6. How many and what types of cyber incidents do we detect in a normal week? What is the threshold for notifying our executive leadership?
7. How mature is our cyber incident response plan? How often is our incident response plan tested and what were the results of the latest test? Does it include a communications strategy?
8. Do we have a relationship with other security personnel in our sector and law enforcement (local, FBI, U.S. Secret Service) that could be leveraged in the event of a breach?
9. How do we monitor cybersecurity risk on an ongoing basis, and what are the key metrics?
10. Do we have cyber-insurance coverage to offset some of our cyber-risk, and what does the policy cover?

Source: Actions to Address Retail Cybersecurity Risk: Considerations for CEOs, NRF and The Chertoff Group, September 2014

Thank You!

Tom Litchford
VP, Retail Technologies
National Retail Federation
litchfordt@nrf.com
202/626.8126

Anatomy of a Large US Retailer Breach



1 The attacker remotely accessed the victim's environment through a virtualized application server. The attacker used valid credentials to authenticate.

2 The attacker broke out of the virtualized application and began moving laterally into the corporate environment. From there, the attacker began harvesting credentials from systems in the environment.

3 The attacker used the retail environment domain controller as a pivot point to the POS registers. From there the attacker deployed card harvesting malware that collected track data from the POS registers.

4 The attacker collected the harvested track data from the POS registers and transferred it from the retail domain controller to a user workstation in the retail environment. The attacker then used FTP to transfer the harvested track data to an external FTP server.

Source: Mandiant M-Trends 2015