Data Breaches and Multiple Points to Stop Them

Danfeng (Daphne) Yao
Professor of Computer Science
Virginia Tech

Waterloo Cybersecurity and Privacy Institute (CPI) 2021

My winding path from nature science to computing

Chemistry degree from Peking University

Quit from Chemistry PhD program in Princeton University

Computer Science Master degree from Indiana University

Computer Science PhD from Brown University

Work in VT College of Engineering for 12+ years

LeShan Budda
（乐山大佛）in 2019

My Product

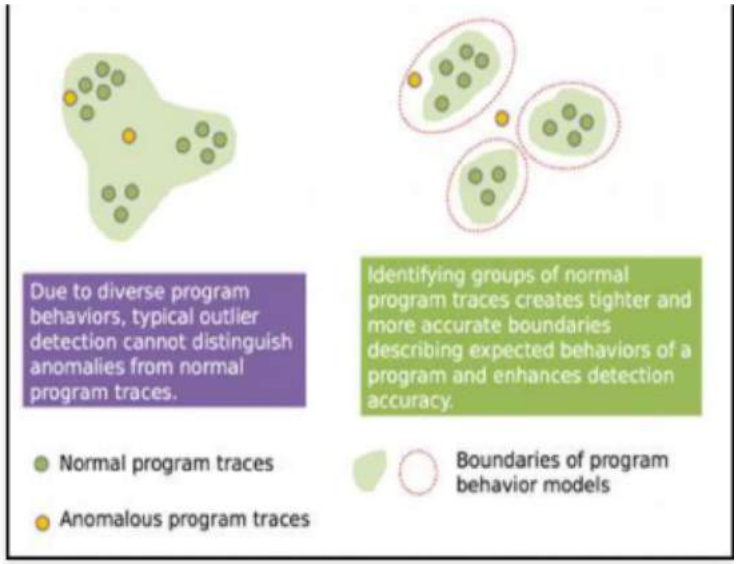
My research and teaching area

SECURING CRYPTO IMPLEMENTATIONS

Software vulnerabilities are costly. NIST estimates that cost to be $60 billion each year, which includes the costs for developing and distributing software patches and reinstalling infected systems and the lost productivity due to malware and errors.

DATA BREACHES AND CERTIFICATION SECURITY

The massive payment card industry (PCI) involves various entities such as merchants, issuer banks, acquirer banks, and card brands. Ensuring security for all entities that process payment card information is a challenging task. The PCI Security Standards Council requires all



PROGRAM AND SYSTEM ANOMALY DETECTION

Program and system anomaly detection analyzes normal program and system behaviors and discovers aberrant executions caused by attacks, misconfigurations, program bugs, and unusual usage patterns. It was first introduced as an analogy between intrusion detection for programs

https://yaogroup.cs.vt.edu/index.html

Our computing professional community is very diverse

Daphne organized CyberW workshop in 2017

Cybersecurity has much more beyond hacking

Computing has much beyond coding

YouTube

Radia Perlman's Fun Keynote at iMentor Workshop

iMentor

Radia Perlman

National Academy of Engineering (NAE) member

Currently at Dell

My Career Journey and Lessons Learned Along the Way

https://sites.google.com/vt.edu/imentor/program

Evolving landscape of attacks

[1980's - early 1990's] Curiosity fueled hacking: capability demonstration of hackers

[late 1990's – present]

Financial driven attacks: spam, stealing credit cards, phishing, large-scale botnets

[Late 2000 – present]

Targeted attacks: stealing proprietary information, information warfare

[2012 – present]

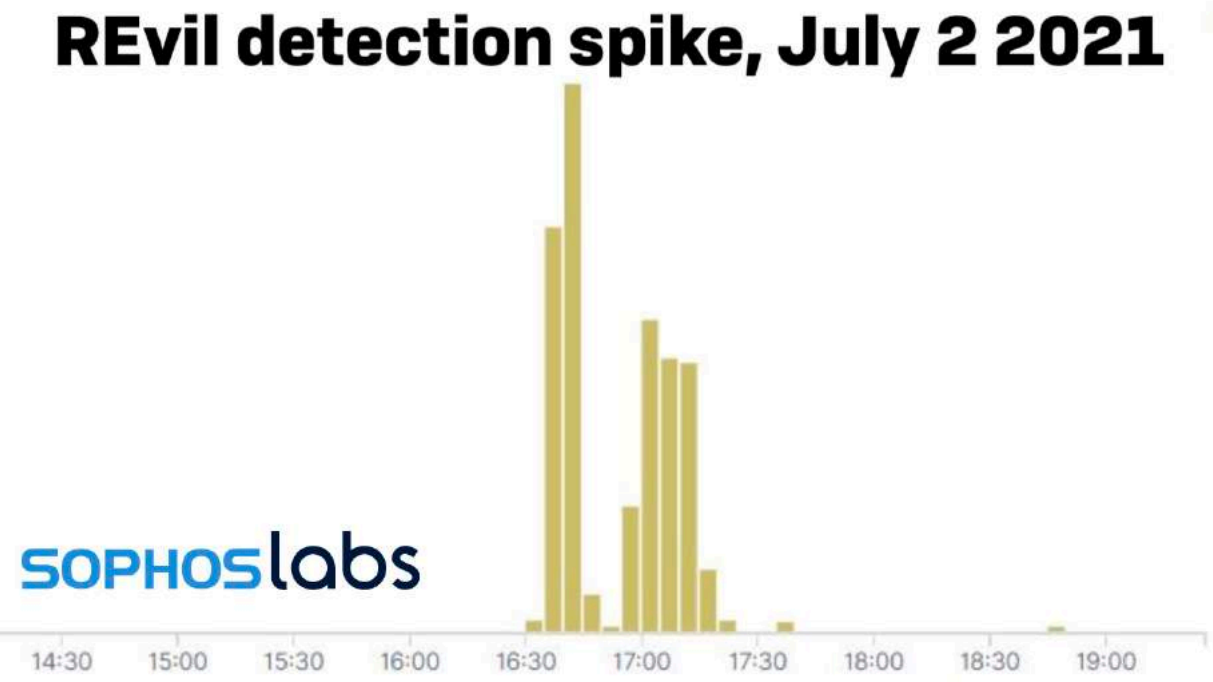
Ransomware, CPS attacks, 0-day supply chain attacks

Challenges caused by:

Scale, complexity, anonymity

"Internet was a friendly place (in the '80s). Security problem then was a day at the beach."
-- Barbara Fraser

Beach days no more ☹



Kaseya Supply-chain attack (2021)

Issued right before Labor Day 2021

https://news.sophos.com/en-us/2021/07/04/independence-day-revil-uses-supply-chain-exploit-to-attack-hundreds-of-businesses/
https://us-cert.cisa.gov/ncas/current-activity/2021/08/31/fbi-cisa-advisory-ransomware-awareness-holidays-and-weekends

CISA, FBI recommend vigilance online to ward off ransomware attacks around Thanksgiving

Three major cyberattacks have occurred around holidays.

By **Luke Barr**
November 24, 2021, 6:35 PM • 4 min read

FBI warns industries of cyberattacks over the holidays

The FBI and Homeland Security told critical industries and businesses to be on the looko... **Read More**

pas/AFP/Getty Images

https://abcnews.go.com/Politics/cisa-fbi-recommend-vigilance-online-ward-off-ransomware/story?id=81354157

Hacking

Ransomware attack on San Francisco public transit gives everyone a free ride

Nov 2016

San Francisco Municipal Transport Agency attacked by hackers who locked up computers and data with 100 bitcoin demand

https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware

VIRGINIA TECH

54,404.00 USD

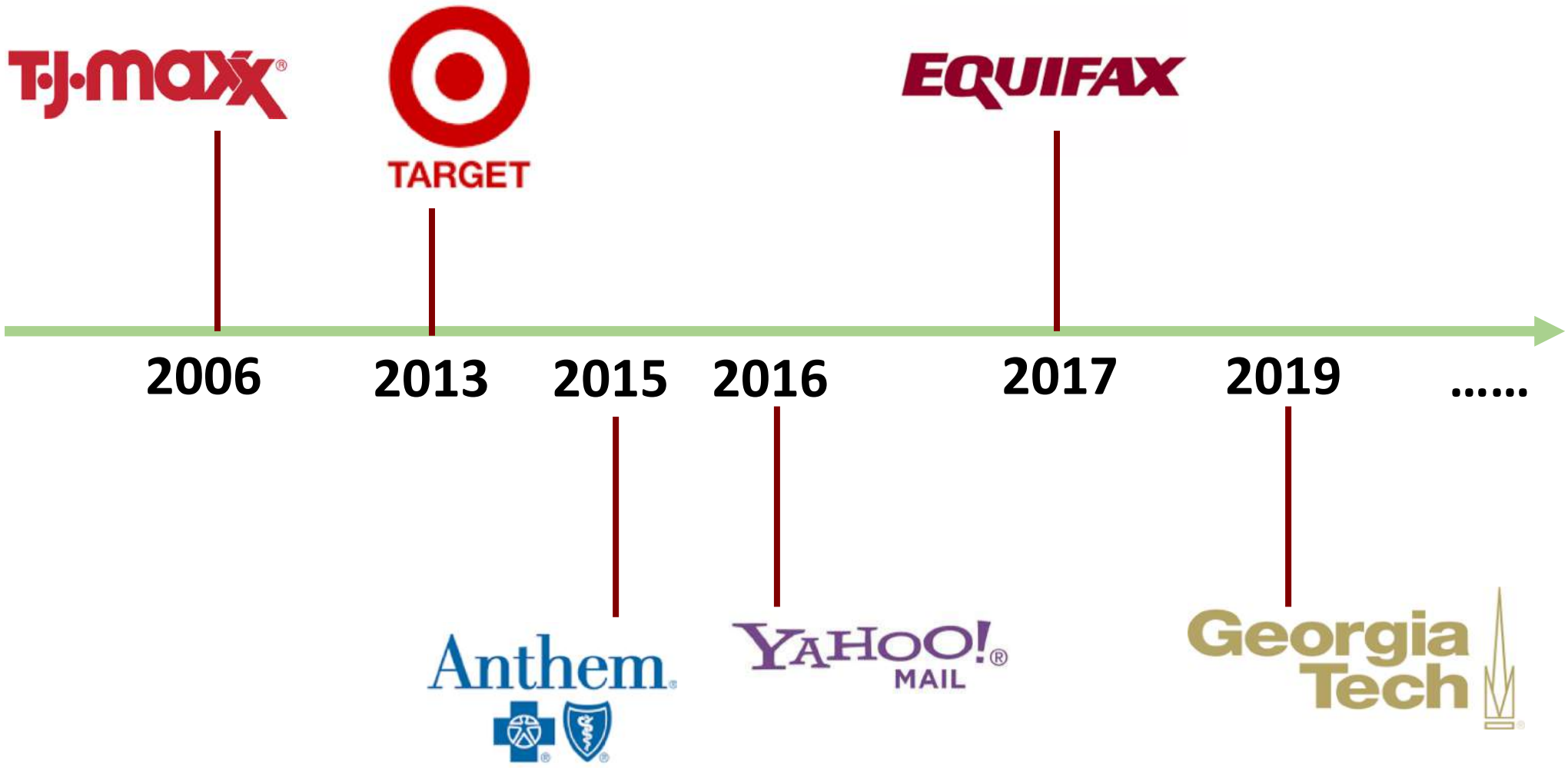
+53,628.13 (6,912.00%) ↑ past 5 years

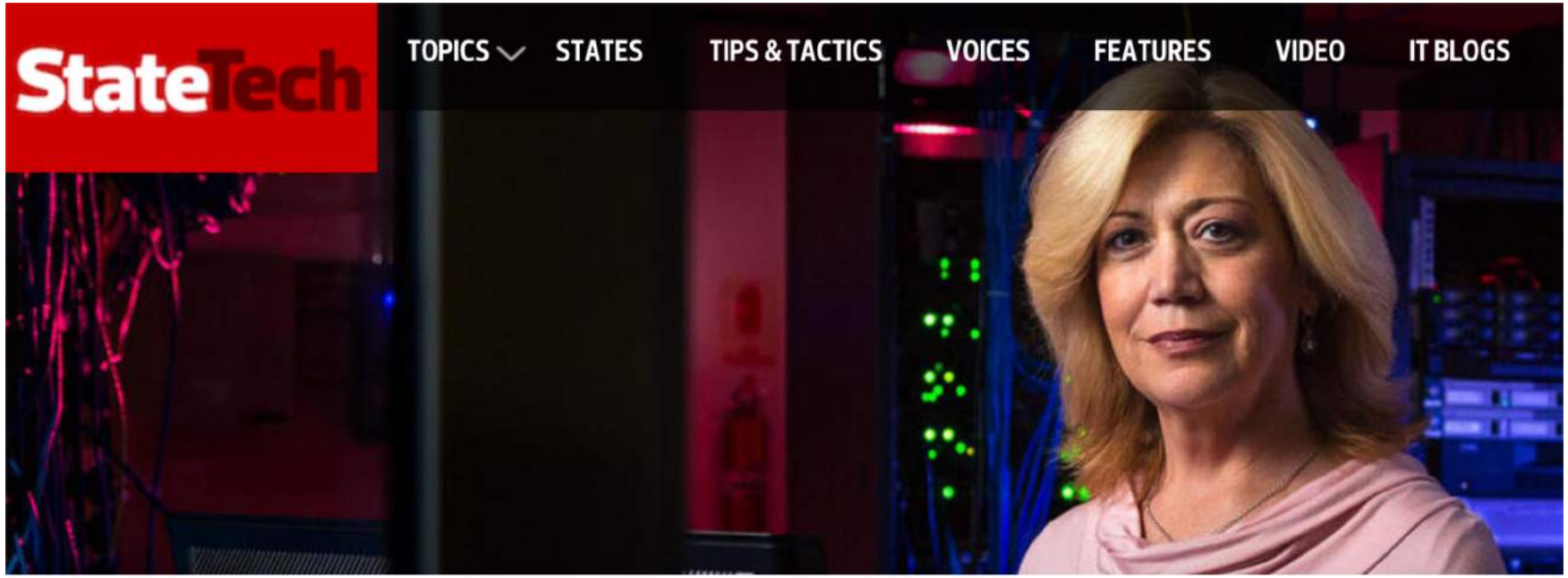
Nov 28, 2:59 AM UTC · From Coinbase and Morningstar · Disclaimer

1D | 5D | 1M | 6M | YTD | 1Y | 5Y | Max

1	BTC	54404.00	USD

My fair share of data breach experiences





HOME >> SECURITY

SECURITY

JAN 31 2017

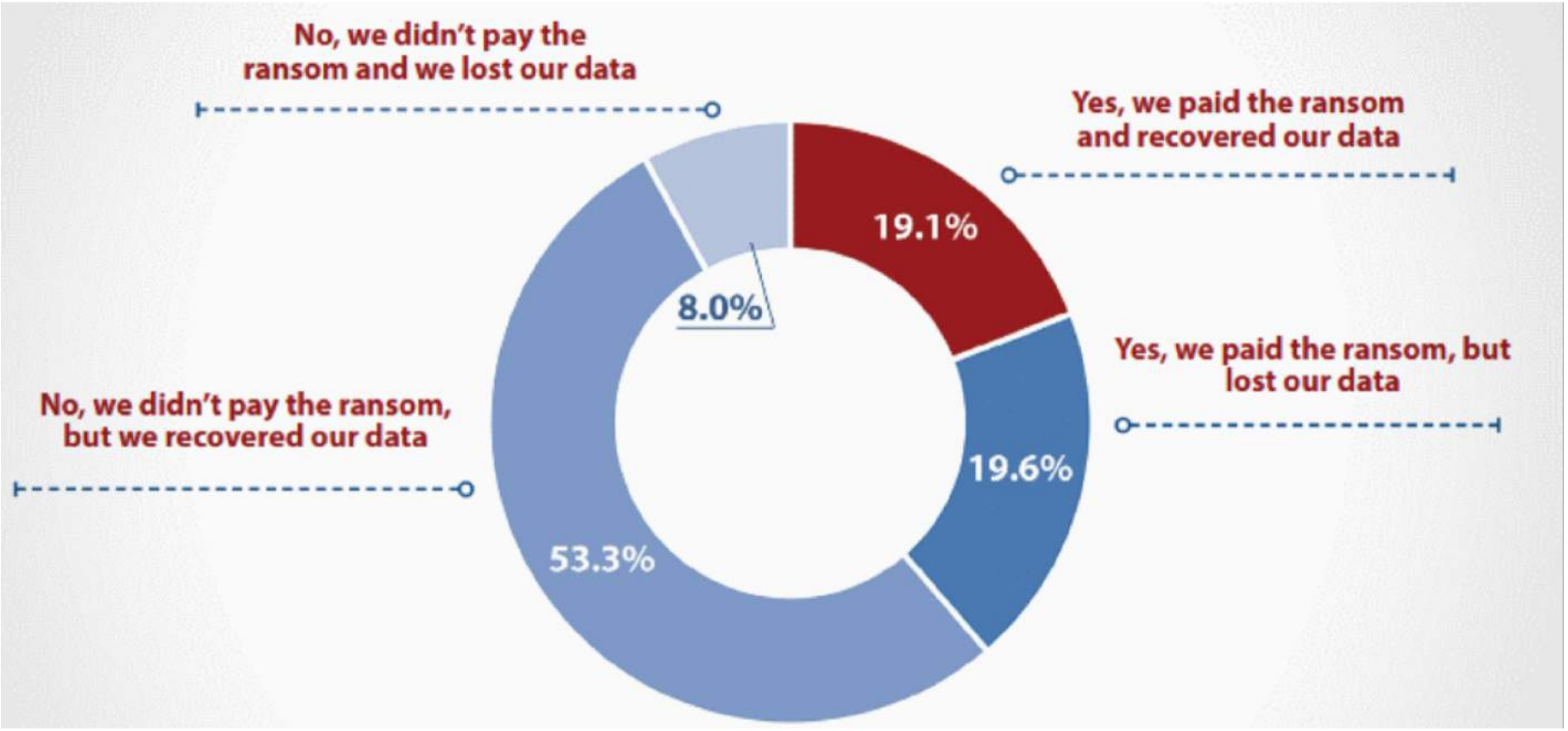
How 3 Local Governments Mitigated Ransomware Attacks

Planning and education help local governments blunt the effects of ransomware attacks.

https://statetechmagazine.com/article/2017/01/how-3-local-governments-mitigated-ransomware-attacks

To pay or not to pay? That's the question

Survey of nearly 1,200 IT security practitioners and decision makers across 17 countries



https://www.bleepingcomputer.com/news/security/only-half-of-those-who-paid-a-ransomware-were-able-to-recover-their-data/

There’s also good news!

Oct. 17, 2021

“Domains hijacked from REvil,” wrote 0_neday, an REvil leader, on a Russian-language forum popular with cyber criminals.

“The server was compromised,” he wrote hours later, “and they are looking for me.”

“Good luck everyone, I’m taking off.”

Ransomware gang shut down after CyberCom hijacked its site and it discovered it had been hacked

BY ELLEN NAKASHIMA AND DALTON BENNETT
NOVEMBER 3 AT 9:16 AM

A major overseas ransomware group shut down last month after a pair of operations by U.S. Cyber Command and a foreign government targeting the criminals’ servers left its leaders too frightened of identification and arrest to stay in business, according to several U.S. officials familiar with the matter.

https://www.washingtonpost.com/national-security/cyber-command-revil-ransomware/2021/11/03/

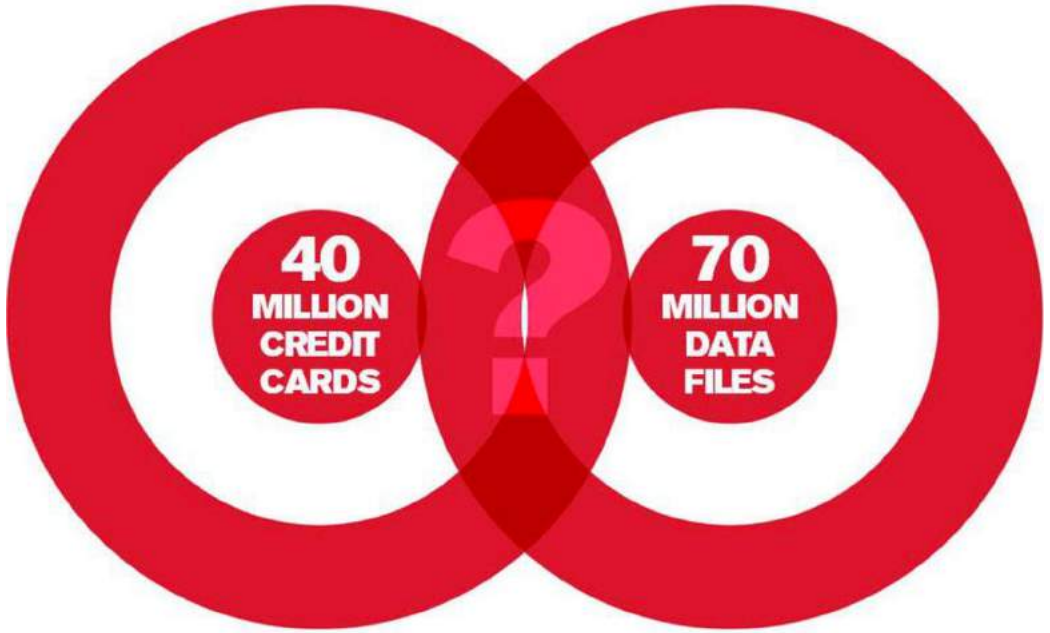
Security is relative. Can you prove it?

You (a hacker) write malware.

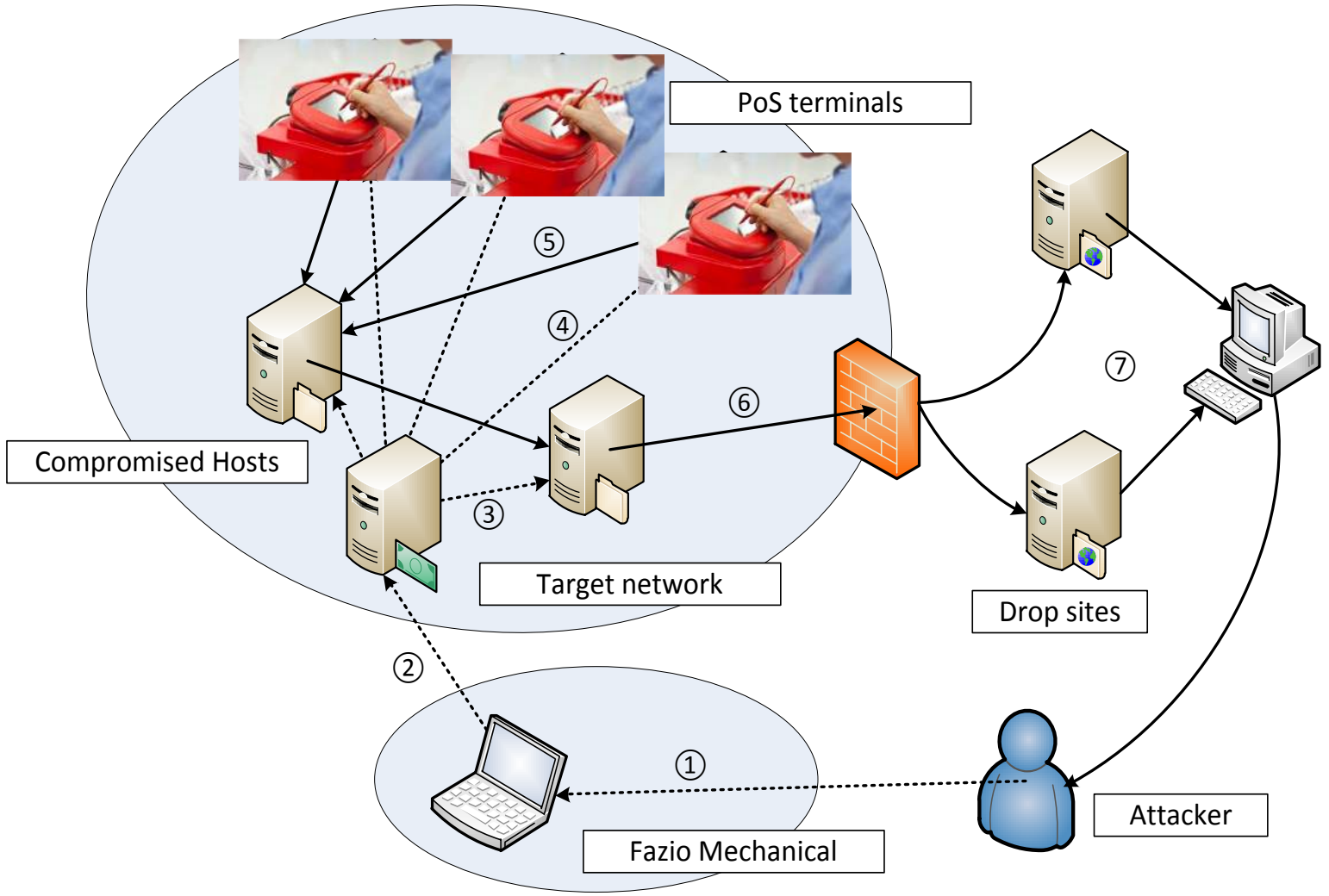
You know most people run Symantec anti-virus (AV) scans.

What would you do before you launch the malware (malicious software)?

Target data breach



Target data breach (Nov. 27 to Dec. 15, 2013)



control path
data flow

1. Phishing attack against Fazio Mechanical Service

2. Accessing the Target network

3. Gaining access to vulnerable machines

4. Installing malware on PoS terminals

5. Collecting card information from PoS

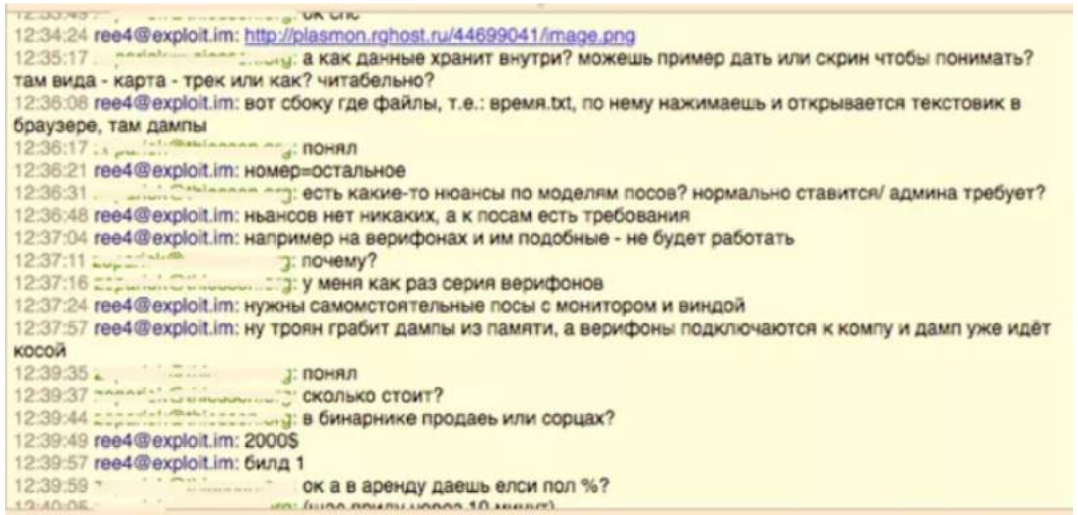
6. Moving data out of the Target network

7. Aggregating stolen card and person data

Breaking the Target. Yao et al. https://arxiv.org/pdf/1701.04940.pdf

ree4@exploit.im: http://plasmon.rghost.ru/44699041/image.png
hidden: how does it keep the data (intercepted credit cards)?
reed4@exploit.im: from left side it is files, time.txt, then you click on it and you will find dumps in browser in plaintext
hidden: are there any differences in terms of infected Point-of-Sale systems?
ree4@exploit.im: no, but there are some nuances, for examples it doesn't work on Verifone
hidden: really? I have Verifones ...
reed4@exploit.im: it grabs dumps from memory, Verifone can be connected to PC, but it will be "secured", you need standalone Point-of-Sale terminals with monitor and Windows
hidden: how much?
ree4@exploit.im: 2000 USD

March 23, 2013



https://securityaffairs.co/wordpress/21337/cyber-crime/blackpos-malware.html

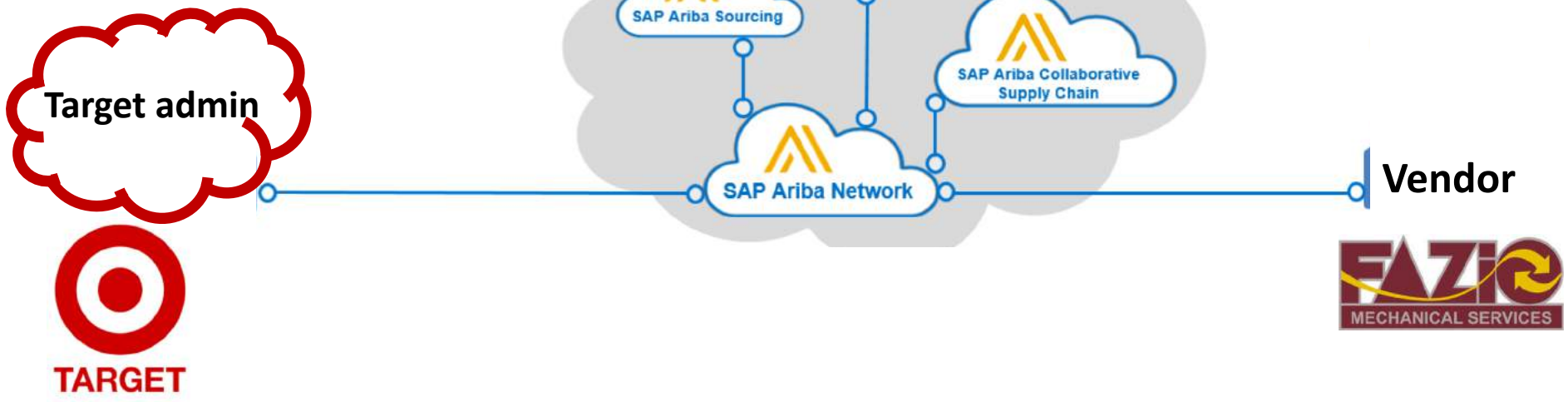
How can a HVAC vendor's credential access Target's internal networks?

"**Fazio Mechanical does not perform remote monitoring of or control of heating, cooling and refrigeration systems for Target**," Fazio said (Feb. 2014).

A Theory

1. Php scripts uploaded as invoices to Target's billing portals

2. Web server attempted to open it; code got executed



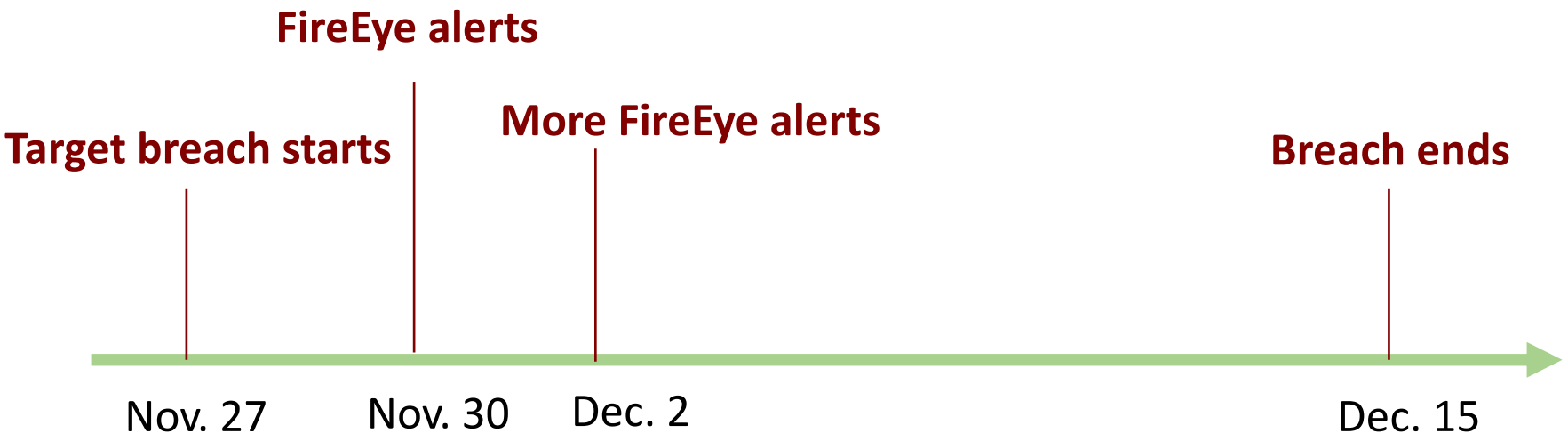
https://www.owasp.org/index.php/Unrestricted_File_Upload

https://aroundcyber.files.wordpress.com/2014/09/aorato-target-report.pdf

Missed opportunities

Lack of transparency makes it difficult to learn from past failures

FireEye's IDS



Target's security team in Bangalore received alerts; sent alerts to Target headquarters

FireEye's auto-malware-delete function was turned off


Palama St
MISSILE ALERT
IN ERROR
THERE IS NO THREAT
EXIT 20
Palama St.
NEXT RIGHT
15'-3"
15'-6"

(Jan. 13, 2

FireEye makes alerts worthwhile again

FireEye

It takes 157 minutes for an expensive expert analyst to correctly identify a true positive alert. That's a lo

- Th **engine** identifies true positive alerts without volumes of alerts or false positives. Since se
  ion leaves them free for more important tasks. It even finds signs of threats for previously u
  tual intelligence accompanies validated alerts to help your analysts quickly prioritize alerts
  s attacker profile, threat severity and attack scale and scope.
  rehensive visibility across the entire lifecycle to reduce alerts by up to 76 percent. By seein
  lerts that would be generated from subsequent stages of the attack (e.g. callbacks) and alerts

157 minutes to confirm a true positive

"We haven't seen any false positives and the alerts e
going on across our whole infrastructure. And by getti
minimize wasting resources on having to clean up a b
posture is even more valuable for us."

- SCOTT ADAMS, MANAGER

Research opportunities:

Better warning design for security analysts

Breaking the Target. Yao et al. https://arxiv.org/pdf/1701.04940.pdf

PCI Compliance is just a baseline

"Target was certified as meeting the standard for the payment card industry (PCI) in Sept. 2013."

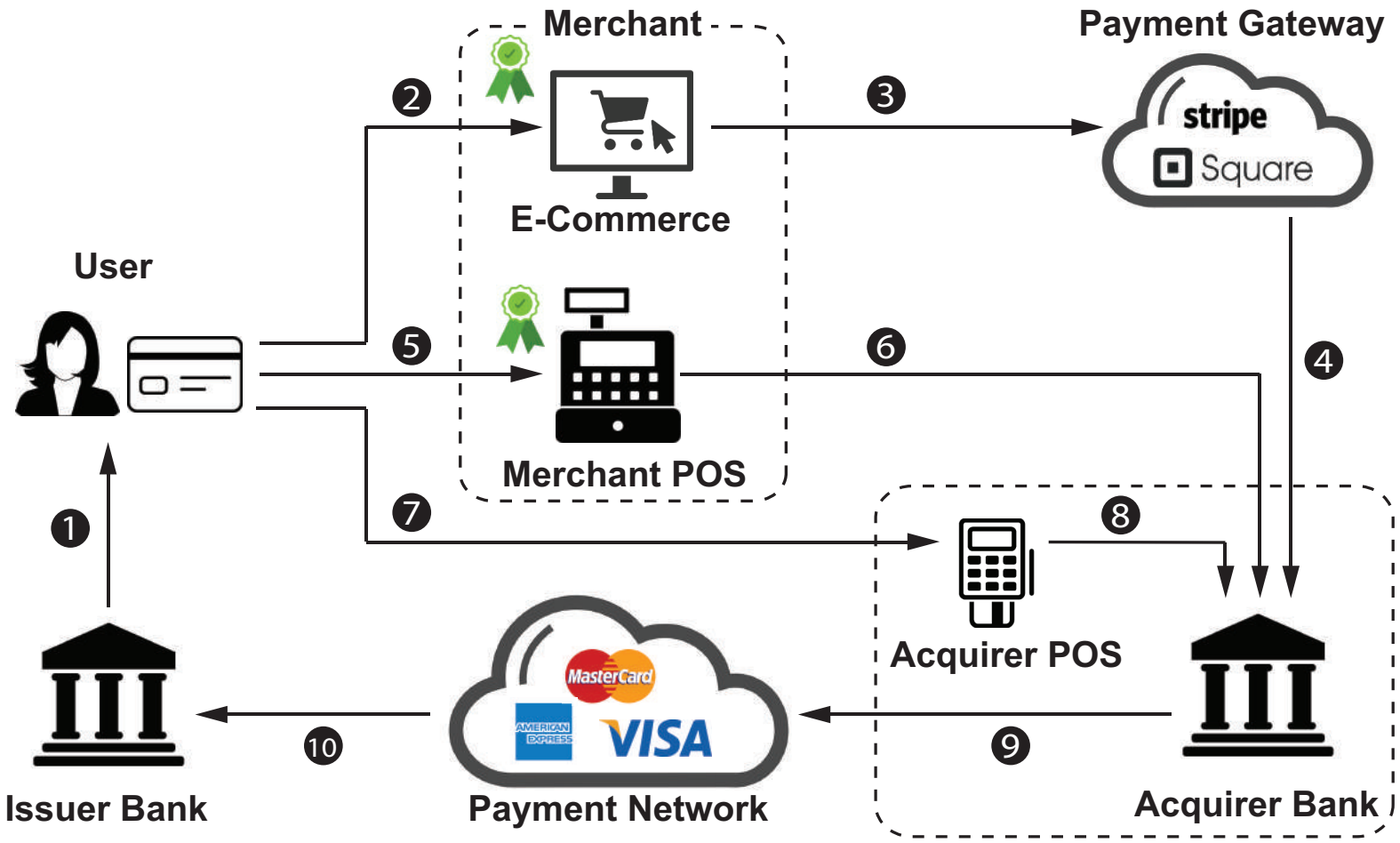
-- Gregg Steinhafel (Target then CEO, stepped down in ‘14)

https://www.pcisecuritystandards.org/

Payment Card Industry (PCI) Security Standard Council Manages All Systems That Touch Payment Cards

PCI data security standard is a standard for securing electronic payments

Payment card ecosystem



VIRGINIA TECH

DISCOVER NETWORK

ATTESTATION OF COMPLIANCE STATUS WITH DISCOVER NETWORK'S SECURITY REQUIREMENTS

Discover Network requires all Merchants, Acquirers, Third Party Processors and Payment Service Providers ("Company") to comply with the Payment Card Industry Data Security Standard ("PCI DSS") located at www.discovernetwork.com and/or www.pcisecuritystandards.org as well as any additional security requirements and all related compliance requirements promulgated by Discover Network from time to time. This document will serve as your attestation of compliance with Discover Network's Security Requirements. The information below must be completed in its entirety, signed by an authorized officer of Company and submitted to Discover Network according to the instructions in Section 5.

Section 1 - Company Contact Information	
Date	
Company Legal Name	
Compliance Contact Name	
Compliance Contact Phone Number	(XXX)XXX-XXXX
Compliance Contact E-mail Address	

Section 2 - Company's PCI Compliance Status	
(Name/Title of Officer) certifies the following compliance status (select one):	
☐ COMPLIANT	(Company) has achieved full compliance with the PCI DSS as of (date of compliance). Name of Qualified Security Assessor (if applicable): **Proceed to Section 4.**
☐ NON-COMPLIANT	(Company) has not achieved full compliance with the PCI DSS as of (date). Company plans to achieve full compliance on: (date). **Company is required to complete Section 3.**

Section 3 - Summary of Company's Compliance with PCI DSS Requirements

Please select the appropriate "Compliance Status" for each requirement. If you answer "NO" to any of the requirements, you are required to provide the date Company will be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

PCI Req.	Description of Requirement	Compliance Status (select one)		Remediation Date and Actions (if "Non-Compliant" was selected in the "Compliance Status" column)
		Compliant	Non-Compliant	
1	Install and maintain a firewall configuration to protect cardholder data	☐	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☐	☐	
3	Protect stored cardholder data	☐	☐	
4	Encrypt transmission of cardholder data across open, public networks			
5	Use and regularly update anti-virus software			
6	Develop and maintain secure systems and applications			
7	Restrict access to card to-know			
8	Assign a unique ID to each person with computer access	☐	☐	

Protect stored cardholder data

Regularly test security systems and processes

Multi-factor authentication -- A lesson learned by PCI from the Target breach

8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.

Note: Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.

8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.

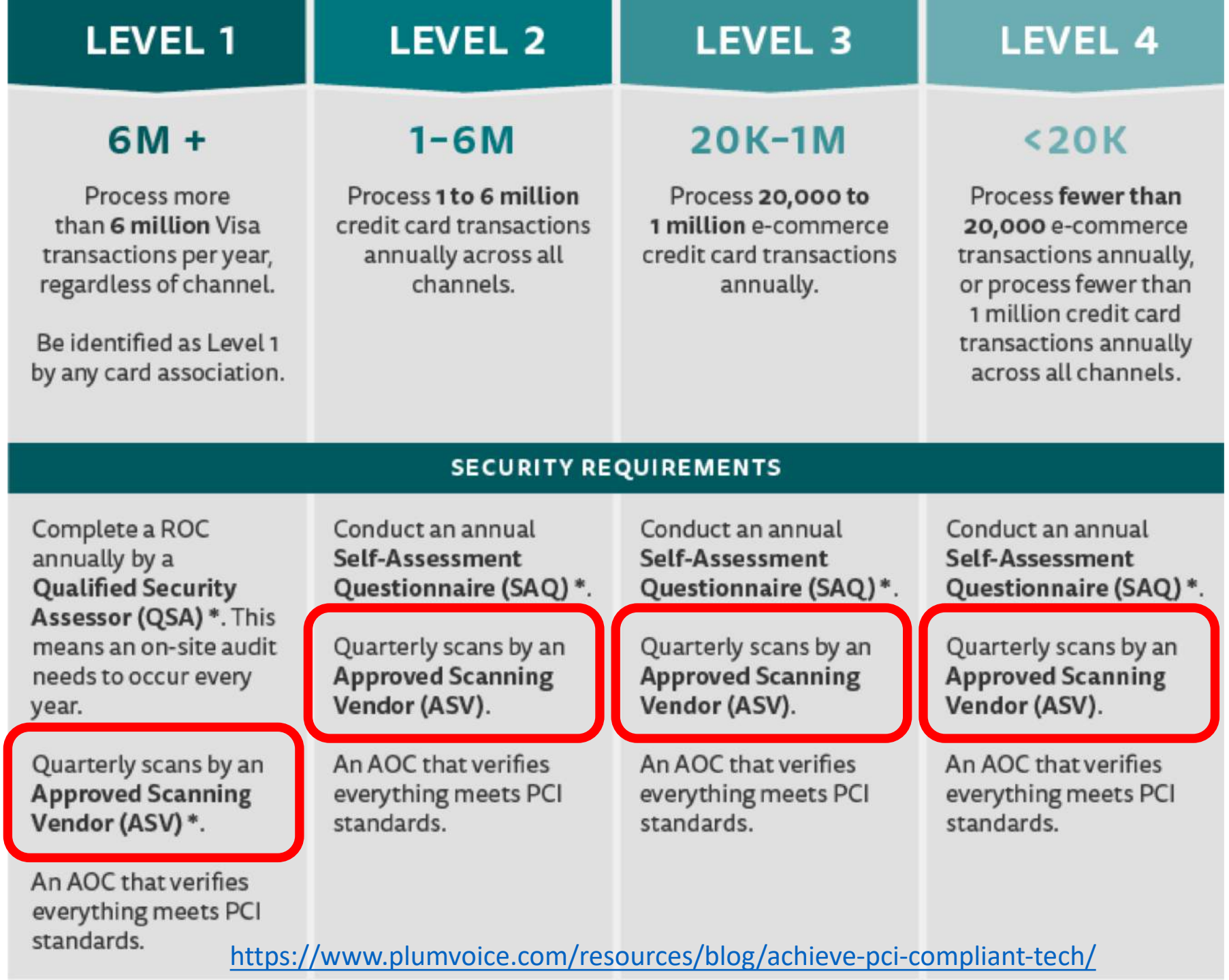
Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.

8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third party access for support or maintenance) originating from outside the entity's network.

https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2.pdf

VIRGINIA TECH

PCI merchant levels



LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
6M +	**1-6M**	**20K-1M**	**<20K**
Process more than **6 million** Visa transactions per year, regardless of channel. Be identified as Level 1 by any card association.	Process **1 to 6 million** credit card transactions annually across all channels.	Process **20,000 to 1 million** e-commerce credit card transactions annually.	Process **fewer than 20,000** e-commerce transactions annually, or process fewer than 1 million credit card transactions annually across all channels.
SECURITY REQUIREMENTS			
Complete a ROC annually by a **Qualified Security Assessor (QSA) ***. This means an on-site audit needs to occur every year.	Conduct an annual **Self-Assessment Questionnaire (SAQ) ***.	Conduct an annual **Self-Assessment Questionnaire (SAQ) ***.	Conduct an annual **Self-Assessment Questionnaire (SAQ) ***.
Quarterly scans by an **Approved Scanning Vendor (ASV) ***.	Quarterly scans by an **Approved Scanning Vendor (ASV)**.	Quarterly scans by an **Approved Scanning Vendor (ASV)**.	Quarterly scans by an **Approved Scanning Vendor (ASV)**.
An AOC that verifies everything meets PCI standards.	An AOC that verifies everything meets PCI standards.	An AOC that verifies everything meets PCI standards.	An AOC that verifies everything meets PCI standards.

https://www.plumvoice.com/resources/blog/achieve-pci-compliant-tech/

Some vendor's scanning capabilities look rather basic

Test Scope

The vulnerability scanning service covers all machines in the given intern ess range from which responses were detected. For each machine det ices an characteristics of the machine are analysed.

TCP/IP characteristics	ICMP responses and stics of the machine are examined. Th he detected operating system (often includi stem uptime where available.
	TCP services and relevant further information is Netcraft's tests identify the network service on each port — in rticular, standard network services running on non-standard ports are identified and fully tested.
UDP services	A table of UDP ports which are believed to be open, and any information obtained from them. Note that due to the design of the UDP protocol, false positives are common in identifying active UDP ports, especially if firewalls are filtering content from these ports. If filtering is in place, our

But security guarantees are often vague

[Source anonymized]

Key Takeaways from Our Study

5 out of 6 PCI scanners

certify vulnerable merchant sites

94% websites (out of 1,203)

Not PCI compliant

[Rahaman, Wang, Yao. ACM CCS 2019]

PCI DSS Specifications are comprehensive, enforcement is tough

Disclosed to the payment card industry security standards council

Target's improvements (April 29, 2014)

Improved monitoring and logging of system activity

Installed application whitelisting POS systems and

Implemented POS management tools

Improved firewall rules and policies

Limited or disabled vendor access to their network

Disabled, reset, or reduced privileges on over 445,000 Target personnel and contractor accounts

Expanded the use of two-factor authentication and password vaults

Trained individuals on password rotation

Target also joined cybersecurity threat-sharing initiatives

FINANCIAL SERVICES Information Sharing and Analysis Center

Financial Services Information Sharing and Analysis Center

R-CISC THE RETAIL ISAC

Retail Cyber Intelligence Sharing Center

US National Cybersecurity and Communications Integration Center

https://www.morganclaypool.com/doi/10.2200/S00800ED1V01Y201709SPT022
https://www.zdnet.com/article/the-target-breach-two-years-later/

https://www.theverge.com/2016/5/6/11601248/nccic-tour-photos-cyber-attack-hq-dhs

Equifax data breach --147 million consumers affected

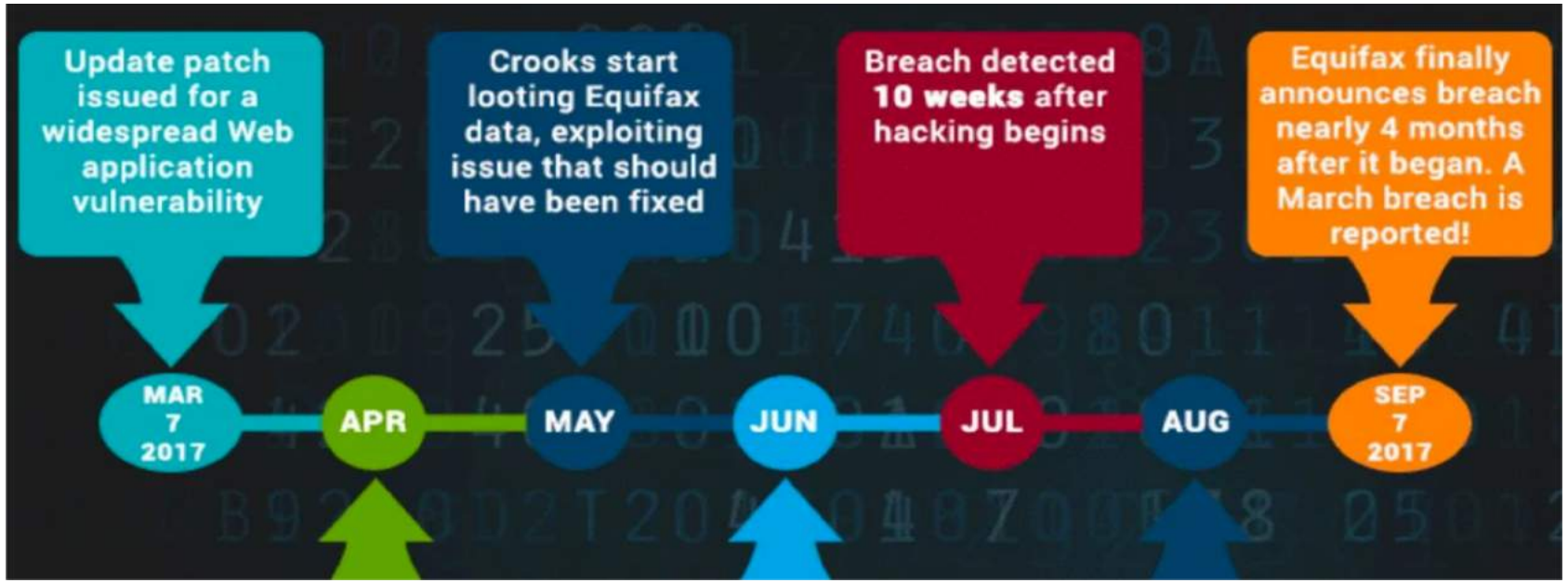
Apache Struts Vulnerability (CVE-2017-5638)

2017-03-06: vulnerability announced on along with a patch

2017-03-07: an exploit released

2017-07-30: Equifax patched

146 days: Time to patch at Equifax



https://www.gracefulsecurity.com/equifax-breach-timeline/
https://blog.blackducksoftware.com/equifax-apache-struts-cve-2017-5638-vulnerability

Vulnerability allows remote attackers to execute commands

```
root@sh:~/struts2-S2-045# python exploit.py http://127.0.0.1:8080/2.3.15.1-showcase/showcase.action "ls -l"
[*] CVE: 2017-5638 - Apache Struts2 S2-045
[*] cmd: ls -l

total 12
lrwxrwxrwx 1 root    root      12 Nov 15 09:37 conf -> /etc/tomcat8
drwxr-xr-x 2 tomcat8 tomcat8 4096 Nov 15 09:37 lib
lrwxrwxrwx 1 root    root      17 Nov 15 09:37 logs -> ../../log/tomcat8
drwxr-xr-x 2 root    root    4096 Mar  7 00:55 policy
drwxrwxr-x 3 tomcat8 tomcat8 4096 Mar  7 01:34 webapps
lrwxrwxrwx 1 root    root      19 Nov 15 09:37 work -> ../../cache/tomcat8
```

Apache Struts: an open-source framework for Java web applications

https://github.com/rapid7/metasploit-framework/issues/8064

Why didn't Equifax patch?

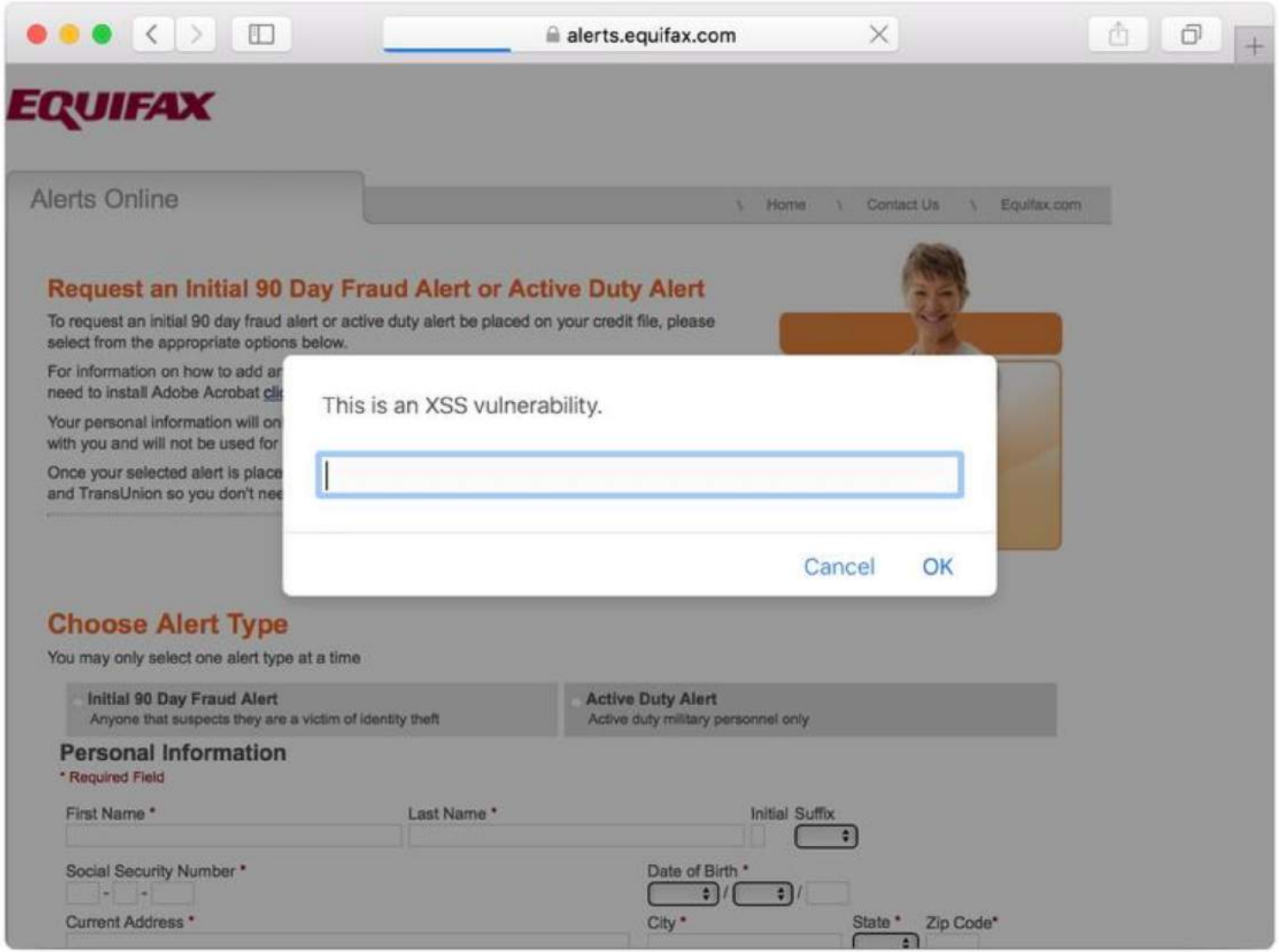
Equifax didn't know what machines run what software – No asset inventory

An "honor system" for patching

A developer didn't receive the vulnerability notice

https://www.hsgac.senate.gov/imo/media/doc/FINAL%20Equifax%20Report.pdf

Cross-site scripting (XSS) Negligence at Equifax



XSS is a well-known web security vulnerability that can be prevented

https://www.netsparker.com/blog/web-security/how-equifax-data-breach-hack-happened/

Equifax's freeze PIN is the timestamp -- predictable

“admin/admin” login for Equifax Argentina employee portal

Id	Apellido	Nombre	Usuario	documento	Email	Estado	Perfil		
1859471	A	Marcela	m		ma ar	INACTIVO	USUARIO	Eliminar	Editar
1859475	A	Yeimy	ya		ye	INACTIVO	USUARIO	Eliminar	Editar
1271524	A	Maria Belen	ba		ma om.ar	INACTIVO	USUARIO	Eliminar	Editar
274804	A	Martin	m		ma	INACTIVO	USUARIO	Eliminar	Editar
527	A	Marita	m		me	INACTIVO	ADMINISTRADOR	Eliminar	Editar
1358701	A	Eugenia	ea		Eu .ar	INACTIVO	USUARIO	Eliminar	Editar
1859467	A	Alejandra	aa		ale .ar	INACTIVO	USUARIO	Eliminar	Editar
1572254	A	Mariela	m		ma	ACTIVO	USUARIO	Eliminar	Editar
2025633	A	Carlos	ca		ca	INACTIVO	USUARIO	Eliminar	Editar
2025667	A	Carlos	ca		ca ar	INACTIVO	USUARIO	Eliminar	Editar
2025660	A	Jose Pablo	jp		Jo	INACTIVO	USUARIO	Eliminar	Editar
709	B n	Marcelo	m		mi	ACTIVO	USUARIO	Eliminar	Editar
1572338	B	Gaston	gb		ga n.ar	INACTIVO	USUARIO	Eliminar	Editar
1789253	B	Priscila	pb	x	pis .ar	INACTIVO	USUARIO	Eliminar	Editar
1536812	B	Martin	m		ma	INACTIVO	USUARIO	Eliminar	Editar
711	B e	Oscar	ob		ob	ACTIVO	USUARIO	Eliminar	Editar
334837	C	Alejandra	ac		ale om.ar	INACTIVO	USUARIO	Eliminar	Editar
123392	C	Guillermo	gc		gu n.ar	INACTIVO	USUARIO	Eliminar	Editar
1433356	D	Laura	ld		lau	INACTIVO	USUARIO	Eliminar	Editar
1702095	D	Eliana	ec		eli r	INACTIVO	USUARIO	Eliminar	Editar

So what? Security is relative anyway.

United States Senate
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
Committee on Homeland Security and Governmental Affairs

Rob Portman, Chairman
Tom Carper, Ranking Member

HOW EQUIFAX NEGLECTED CYBERSECURITY AND SUFFERED A DEVASTATING DATA BREACH

STAFF REPORT

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

UNITED STATES SENATE

https://www.hsgac.senate.gov/imo/media/doc/FINAL%20Equifax%20Report.pdf

Subcommittee concludes:

Equifax's response to the 2017 Apache vulnerability was inadequate ☹

Equifax's broader culture of complacency toward cybersecurity preparedness ☹☹☹

Equifax's shortcomings are long-standing ☹☹

8.5K unpatched bugs found in a 2015 audit 😱😱😱

https://www.hsgac.senate.gov/imo/media/doc/FINAL%20Equifax%20Report.pdf

Many Opportunities to Stop Data Breaches

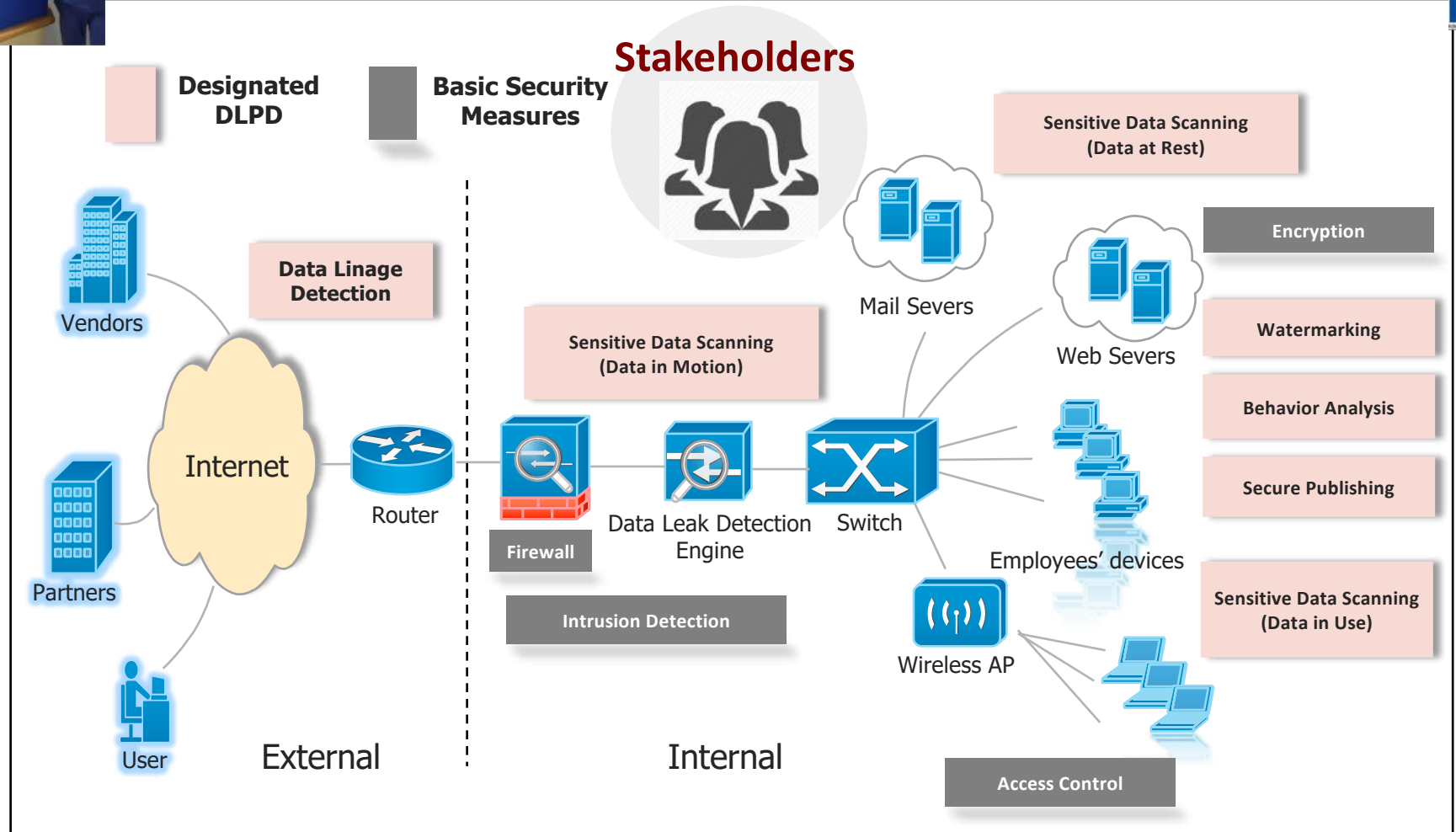
Decision makers

Security analysts

Users

Developers

Regulators



Also, do not collect data that you do not need

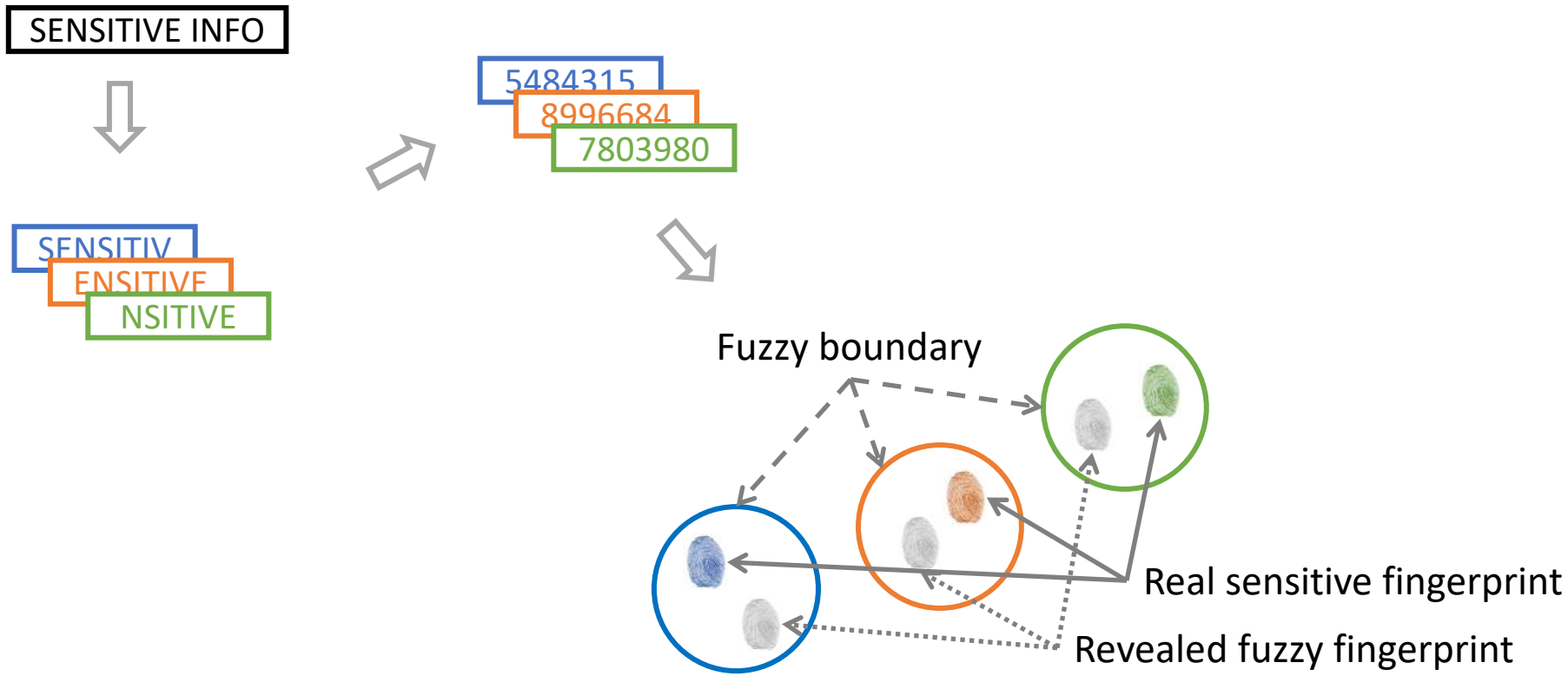
From “Privacy Research that Matters”
by Drs. Jen Whitson and Ian Goldberg

https://www.youtube.com/watch?v=fJ99WGzL3F0

Data Leak Detection as a Service

Threat model: accidental data leak

Our Twist -- Fuzzy Fingerprints



[Shu, Yao, and Bertino. *IEEE TIFS* '15]

Top 25 most downloaded article of IEEE Signal Processing Society in 2018

A follow-up work of mine: Detection of transformed accidental data leak

Auto-formatting (WordPress)

```
The application layer contains the higher-level protocols used by most applications for network communication. Examples of application layer protocols include the File Transfer Protocol (FTP) and the Simple Mail Transfer Protocol (SMTP).[19] Data coded according to application layer protocols are then encapsulated into one or (occasionally) more transport layer protocols (such as TCP or UDP), which in turn use lower layer protocols to effect actual data transfer.

The+application+layer+contains+the+higher-level+protocols+used+by+most+applications+for+network+communication.+Examples+of+application+layer+protocols+include+the+File+Transfer+Protocol+(FTP)+and+the+Simple+Mail+Transfer+Protocol+(SMTP).[19]+Data+coded+according+to+application+layer+protocols+are+then+encapsulated+into+one+or+(occasionally)+more+transport+layer+protocols+(such+as+TCP+or+UDP),+which+in+turn+use+lower+layer+protocols+to+effect+actual+data+transfer.
```

Partial source code leak

```
def encode(msg, pubkey, verbose=False):
    chunksize = int(log(pubkey.modulus, 256))
    outchunk = chunksize + 1
    outfmt = '%%0%dx' % (outchunk * 2,)
    bmsg = msg if isinstance(msg, binary_type) else msg
    result = []
    for start in range_func(0, len(bmsg), chunksize):
        chunk = bmsg[start:start + chunksize]
        chunk += b'\x00' * (chunksize - len(chunk))
        plain = int(hexlify(chunk), 16)
        coded = pow(plain, *pubkey)
        bcoded = unhexlify((outfmt % coded).encode())
        if verbose:
            print('Encode:', chunksize, chunk, plain, c
        result.append(bcoded)
```

[Shu, et al. *IEEE TIFS 2016*]

What should executives do?

What executives should do --

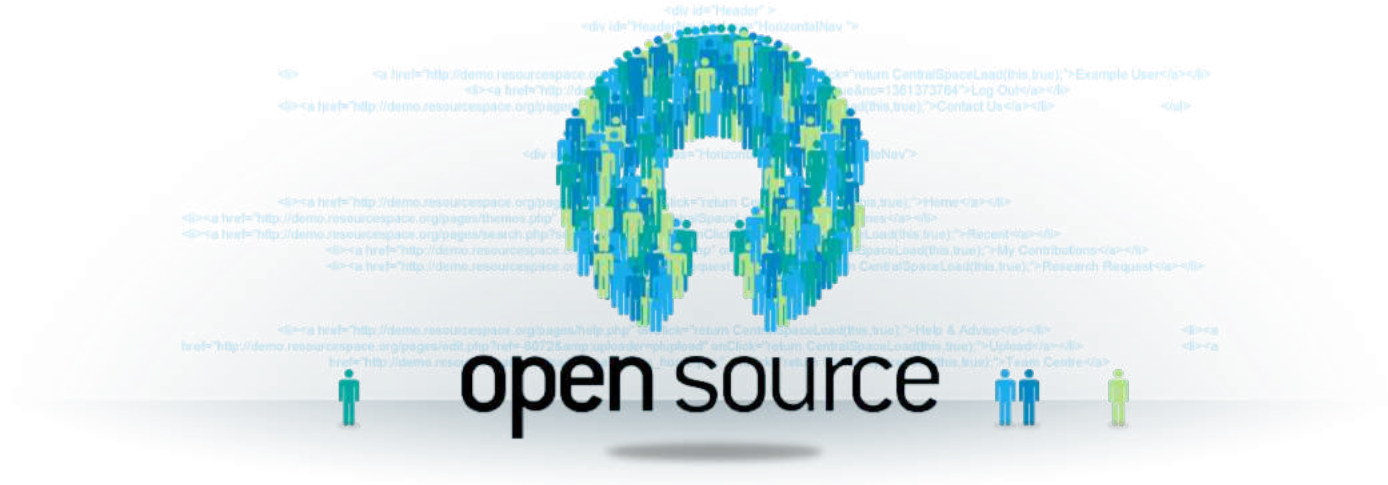
To invest in cybersecurity

Most senior managers who oversaw Equifax cybersecurity in 2017 did not attend Equifax's Global Threats and Vulnerability Management meetings ☹

https://www.hsgac.senate.gov/imo/media/doc/FINAL%20Equifax%20Report.pdf

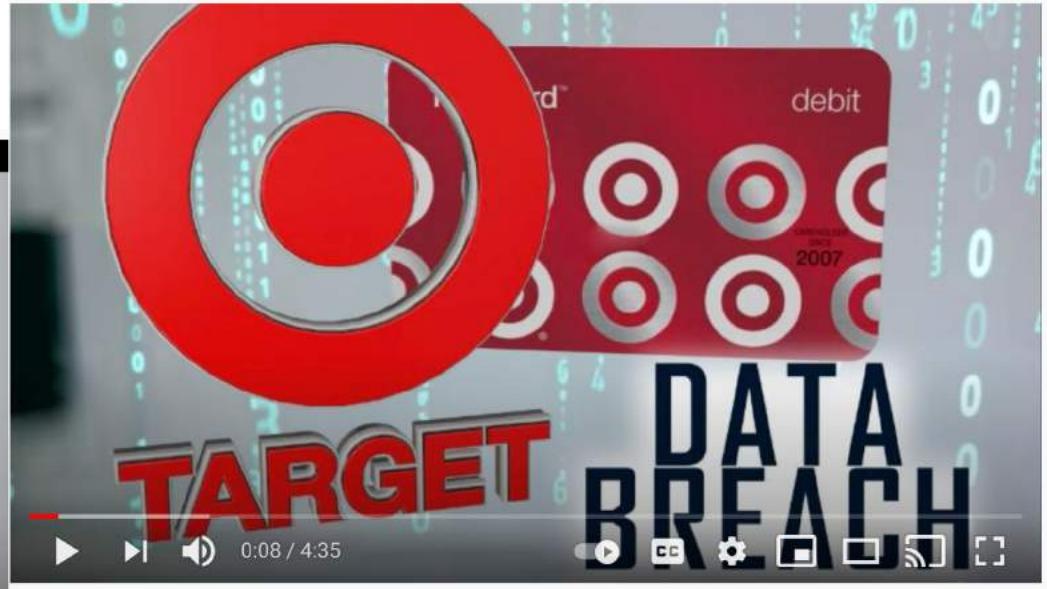
What should researchers do?

What researchers could do?
To bring in transparency and science



YouTube videos on security breaches (Yao group)

Colonial Pipeline Hack (2021) and Ransomware Explained



Target 2013 Data Breach Explained

Video credits:

- **Deepti Suresh**
- **Karla Estrada**
- **Catherine Yue**

https://www.youtube.com/watch?v=CtAXbuv2Hl8
https://www.youtube.com/watch?v=fJtzO2OTBFU
https://www.youtube.com/watch?v=1iPaKSzrSTA&t=6s

Equifax 2017 Data Breach Explained

Cybersecurity has much more beyond hacking

Computing has much beyond coding

Thank you!

danfeng@vt.edu