Protecting Data and Cyber Security

Data incident at the Missouri State Employees' Retirement System

The Incident

- An unauthorized person logged into four user accounts and attempted to set up an Electronic Fund Transfer (EFT) for each account last November and December 2014.
- That person(s) had access to each member's Social Security Number (or Member ID number) and password.
- No loss of funds because the members were not receiving retirement benefits.

The Incident, cont.

- We became aware of the problem after the fact through an automated internal exception report that identified the unsuccessful attempt to set up an EFT for members who were not receiving retirement benefits.
- Members also contacted us after they received EFT confirmation letters.

Statutory Notification

- Section 407.1500 requires: “Any person…that conducts business in Missouri that owns…personal information in any form of a resident of Missouri shall provide notice to the affected consumer that there has been a breach of security following discovery…of the breach…”
- “Breach” – “unauthorized access to…personal information maintained in a computerized form by a person that compromises the security, confidentiality, or integrity of personal information.”

Statutory Notification, cont.

- At a minimum, the notice shall include a description of the incident in general terms, a telephone number that the **affected consumer** may call for further information, contact information for consumer reporting agencies, and advice that directs the consumer to remain vigilant by reviewing account statements and obtaining free credit reports.
- Notice may be by mail, sent electronically, or by provided by telephone.

Initial Staff Reaction

- Were there other members affected beyond the 4 members we knew about?
- Overreaction v. under reaction
- Decision was made to take MOSERS website down on December 11, 2014, and invalidate the credentials for all user accounts.
- Contacted the four affected members by phone.
- Notified members of the incident by email (81,067) or letter if no email address (18,236).

Initial Staff Reaction, cont.

- We did not notify members who had never accessed their online account.
- Notified major credit bureaus of the incident as well as the Office of the Attorney General and participating employers in our plan.
- Notified the Board of Trustees very early in the process and have continued to update them at subsequent board meetings.

Managing the Incident

- MOSERS Business Continuity Steering Committee (BCP) coordinated MOSERS response to this incident
  - Established a Security Response Team (SRT) to identify and coordinate actions required specifically regarding the following areas:
    - Statutory requirements.
    - IT.
    - Communication plan regarding staff, MOSERS members, and the press.
    - Benefits challenges regarding member concerns and a significant increase in workload.

Managing the Incident, cont.

- Developed strategy for communicating with members and the press.
- We designated a detailed note taker who memorialized internal discussions/decisions that took place at meetings involving Benefits, IT, and Communications.
- We created a file on a shared drive that staff could access to get updates on current decisions and strategies to deal with the incident.

Managing the Incident, cont.

- It was critical to keep internal staff informed of news releases, communication to our members, and details of the process developed for the password reset.
- Documented actions taken and conducting a final review process to capture lessons learned.

Communications Section Challenges and the Media

- We issued a statement on our website that provided details of the incident which was picked up by a number of local news sources.
- Press reports mostly reiterated the information we provided on our website.
- Communications coordinator took press calls from the local newspaper, three local TV stations, and radio newsrooms.
- MOSERS benefited from a positive relationship with a local paper based on prior editorial board meetings.

Communication Section Challenges and the Media, cont.

- The executive director declined on-camera interviews with the TV stations. Local TV stations did use recorded conversations with the communications coordinator.
- The communications coordinator created a list of talking points for these interviews and shared them with the reporters.
- <u>Three key points</u> – 1) No money was fraudulently transferred, 2) strong security measures we had in place detected the suspicious activity, and 3) monthly benefit payments would continue on time and in full.
- There was not much to report after the initial news release.

Password Reset

- The website was brought back online on December 16, 2014.
- Members registered for a new password using a process that required the member to enter a temporary code from MOSERS sent by email.
- If a member's email address was not valid (or in existence), members were required to call and provide a valid email address.
- Absent a valid email address, members were not allowed online access.

Password Reset, cont.

- Having a valid email address also ensured that members would receive notification each time their member homepage was accessed.
- Revised security questions (which needed to be updated anyway).

Benefit Section Challenges

- Once members heard about the incident, calls started.
- Many members misunderstood the notice and assumed their account was affected because they received the notice.
- Once we cleared that up, our biggest challenge was successfully getting the temporary code to our members.
- Some internet service providers (ISPs) blocked our emails through their spam filters – our IT section worked with various ISPs to allow our emails to be delivered.

Benefit Section Challenges, cont.

- We also changed the email subject line to something less likely to trigger a spam filter.
- Initially the temporary password was only valid for 15 minutes – that caused many problems as members needed more time to retrieve the temporary password and enter it into the browser window to complete the reset.
- Ultimately we made the temporary password valid for 6 hours to address these issues.
- Our call volume increased by 62%.

Benefit Section Challenges, cont.

- The length of calls increased by 50%.
- For every six members who did the reset, 1 of them called for assistance.
- Total calls related to the reset/breach: 4,474
- The 4,474 calls we received represented 5% of our total membership (but it seemed like 100% of our members were calling at the time).
- These statistics don't take into account emails sent by members.

Benefit Section Challenges, cont.

- 47% of our members have reset their password.
- Some members were not computer savvy (had difficulty doing the password reset) and likely do not use software to protect against malware, etc.
- High level of stress for the organization but particularly for our benefit counselors who had to communicate directly with members regarding the incident and password reset process.
- …while doing their regular work in assisting members with retirement, etc.

IT Section Challenges

- Identifying the affected members.
- Investigating the incident, running queries, and trying to define the scope of the problem (audit logs, ISP addresses, bank routing numbers, and bank account numbers).
- Changing password reset process on the website with limited time for development and testing.
- Training benefit counselors on changes so they could respond to members.

IT Section Challenges, cont.

- Implementing a form of secondary authentication using email (without the benefit of using cell phone numbers instead).
- We plan on collecting cell phone numbers in the future to use in place of emails for secondary authentication + other forms of communication. Should be a more reliable form of communication than email.

Law Enforcement Contact

- MOSERS Chief Auditor acted as the point of contact for MOSERS.
- The only law enforcement point of contact needed was the cyber-crime division of the Missouri Highway Patrol (MHP) – MHP can coordinate with other law enforcement agencies such as the FBI or local law enforcement.
- After receiving ISP information and login data, MHP obtained a search warrant and served a household in a neighboring rural county. MHP seized a computer that was the last point of contact before the unauthorized person accessed member accounts.

Law Enforcement Contact, cont.

- The family who owned the computer had no idea what was going on and MHP reported that the computer was old and unprotected from spyware and malware.
- MHP was not able to provide much closure but indicated that the debit cards used in the incident were inactive but were previously used to withdraw funds from a bank in Russia.

IT Audit

- MOSERS hired a company called Mandiant to conduct an investigation of MOSERS's networks and to identify any additional evidence of attacker activity.
- Mandiant did not identify evidence of a targeted intrusion of MOSERS's corporate environment.
- Some malware was found (which was remediated) but it was not related to the incident.
- Speculation that access was through external means involving some type of malware.

Conclusions

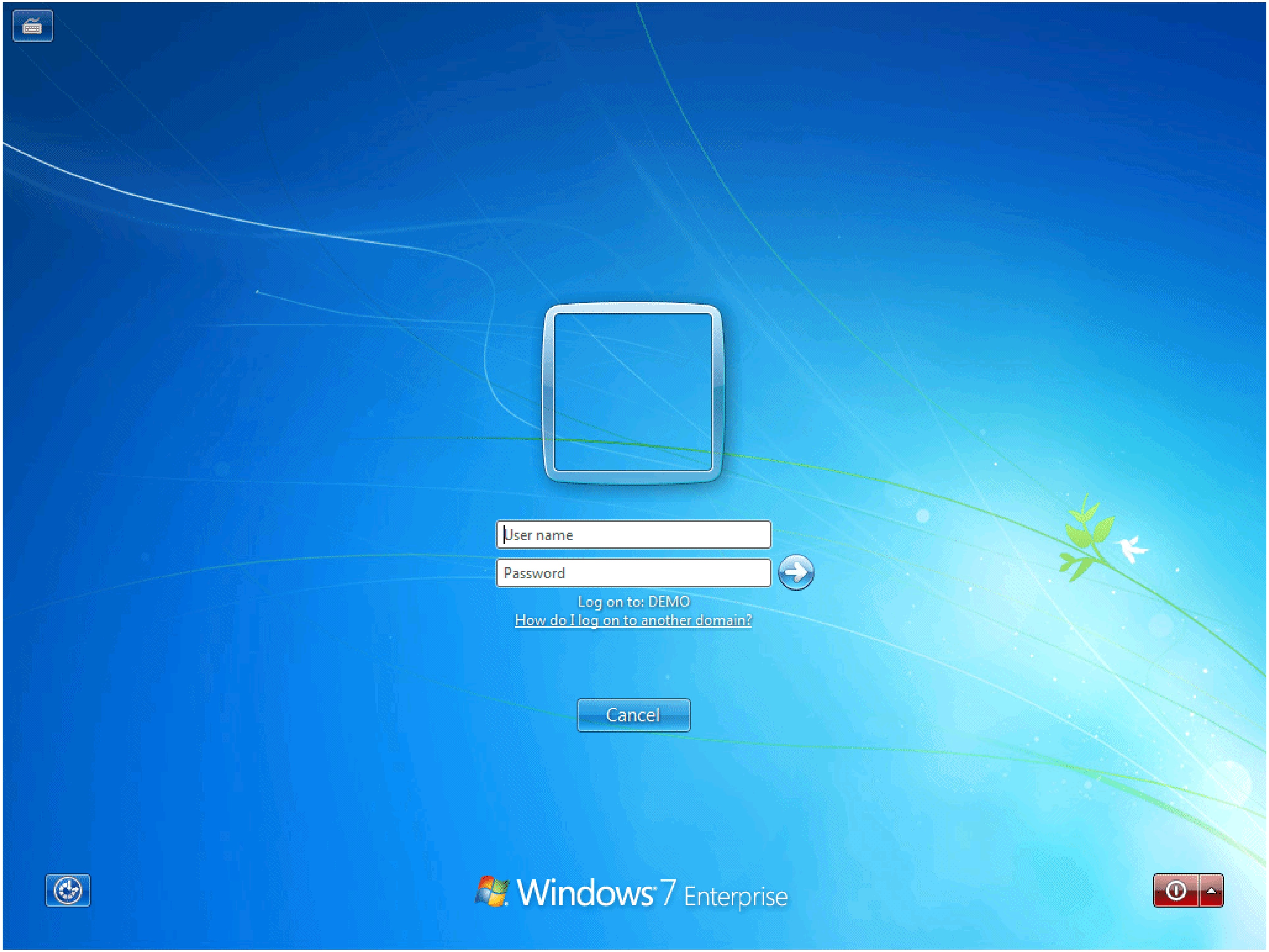
- There is value in being proactive and anticipate security risks and develop strategies to minimize that risk.
- Develop procedures for handling security incidents with Benefits, IT, and Communications.
- Consider making the process part of your disaster recovery plan.
- Member education regarding security.

* Protecting Data & Cyber Security

Brian Farrar
Network Operations Manager
Texas Municipal Retirement System

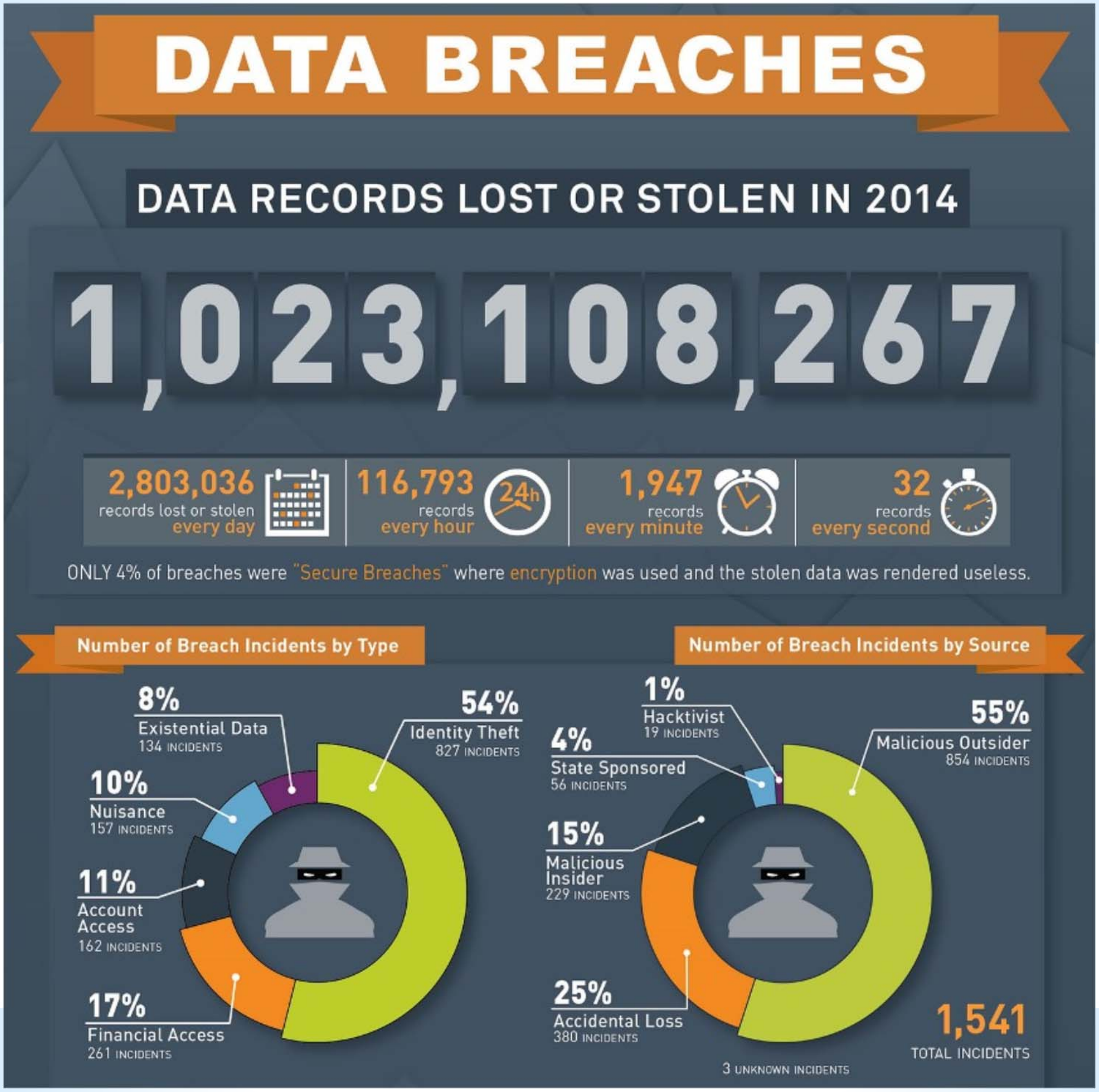
* What keeps me up at night

- Security Breaches
- Advanced Persistent Threats (APT)
- Malware/Ransomware
- Security and You
- Data Loss Prevention (DLP)


User name
Password
Log on to: DEMO
How do I log on to another domain?
Cancel
Windows 7 Enterprise


Hacked By #GOP
Warning :
We've already warned you, and this is just a beginning.
We continue till our request be met.
We've obtained all your internal data including your secrets and top secre
If you don't obey us, we'll release data shown below to the world.
Determine what will you do till November the 24th, 11:00 PM(GMT).
Data Link :
https://www.sonypicturesstockfootage.com/SPEData.zip
http://dmiplaewh36.spe.sony.com/SPEData.zip
http://www.ntcnt.ru/SPEData.zip
http://www.thammasatpress.com/SPEData.zip
http://moodle.universidadebematech.com.br/SPEData.zip


Security Breaches Hit Retailers
THE HOME DEPOT
56M Cards
TARGET
40M Cards
Michaels
2.6M Cards
Neiman Marcus
350,000 Cards
Bloomberg

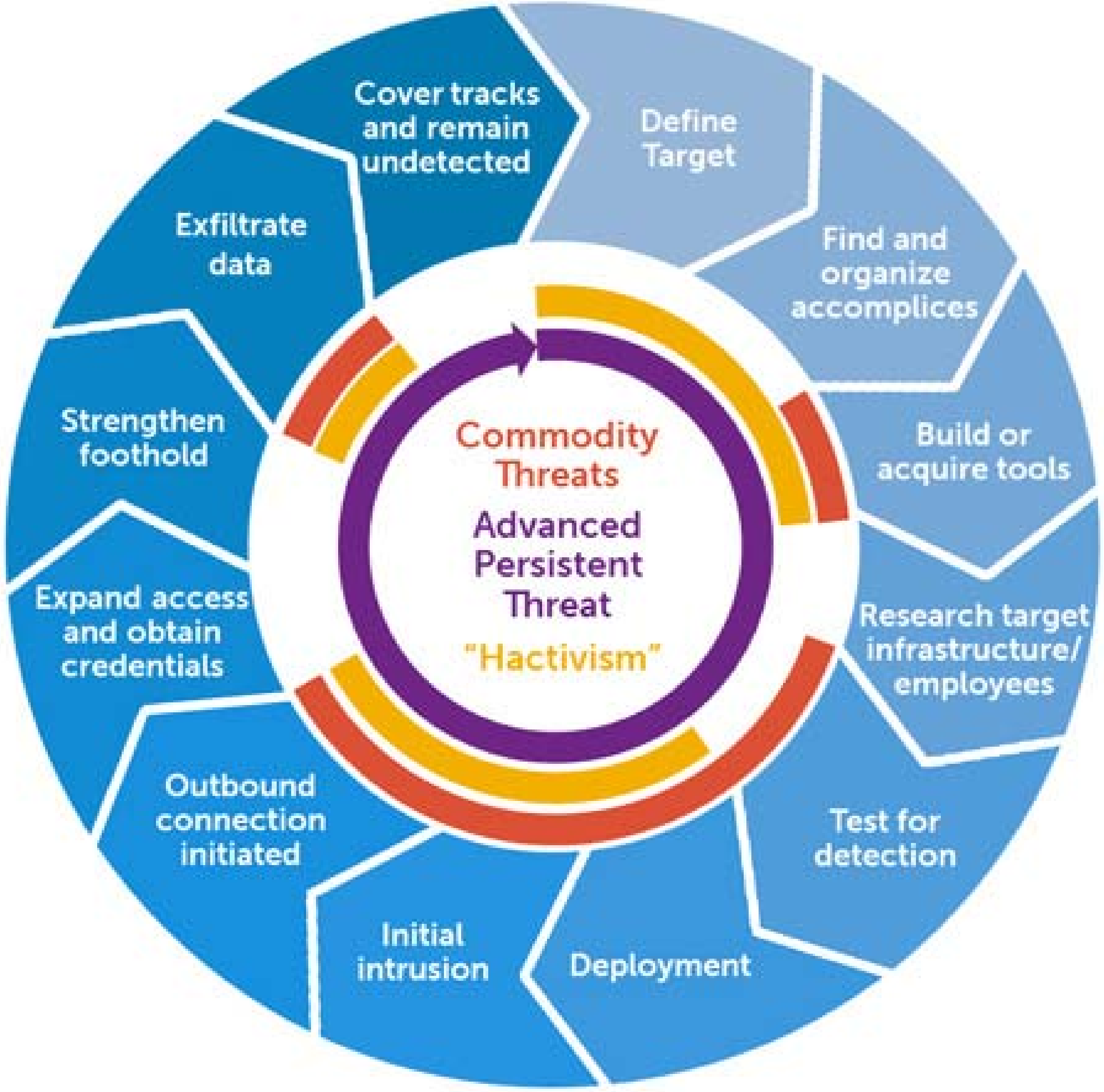

DATA BREACHES
DATA RECORDS LOST OR STOLEN IN 2014
1,023,108,267
2,803,036 records lost or stolen every day
116,793 records every hour
24h
1,947 records every minute
32 records every second
ONLY 4% of breaches were "Secure Breaches" where encryption was used and the stolen data was rendered useless.
Number of Breach Incidents by Type
8% Existential Data 134 INCIDENTS
54% Identity Theft 827 INCIDENTS
10% Nuisance 157 INCIDENTS
11% Account Access 162 INCIDENTS
17% Financial Access 261 INCIDENTS
Number of Breach Incidents by Source
1% Hacktivist 19 INCIDENTS
4% State Sponsored 56 INCIDENTS
55% Malicious Outsider 854 INCIDENTS
15% Malicious Insider 229 INCIDENTS
25% Accidental Loss 380 INCIDENTS
1,541 TOTAL INCIDENTS
3 UNKNOWN INCIDENTS

Data Records Lost/Stolen by Industry
55%
Retail
567,316,824
RECORDS
20%
Financial
205,175,846
RECORDS
9%
Technology
96,493,092
RECORDS
5%
Education
51,377,801
RECORDS
5%
Government
42,844,710
RECORDS
3%
Other
30,515,427
RECORDS
3%
Healthcare
29,384,567
RECORDS
Breach by Region*
1,164
190
38
129
12
North America
1,164 INCIDENTS (76%)
United States 1,107 INCIDENTS
Canada 57
Latin America
12 INCIDENTS (<1%)
Brazil 3 INCIDENTS
Dominican Republic 2
7 other countries
Europe
190 INCIDENTS (12%)
United Kingdom 117 INCIDENTS
France 9
Ireland 8
Germany 7
Netherlands 6
Belgium 5
Russia 3
Italy 3
Denmark 3
Poland 2
Norway 2
Romania 2
Sweden 2
Switzerland 2
Ukraine 2
11 other countries
Middle East/Africa
38 INCIDENTS (<3%)
Turkey 5 INCIDENTS
South Africa 4
Nigeria 2
UAE 2
9 other countries
Asia/Pacific
129 INCIDENTS (8%)
Australia 30 INCIDENTS
China 17
New Zealand 13
South Korea 12
Japan 11
Vietnam 9
India 7
Pakistan 7
Hong Kong 4
Malaysia 4
Azerbaijan 2
Nepal 2
Singapore 2
Taiwan 2
7 other countries
Global 4 INCIDENTS <1%
United Nations 1 INCIDENT <1%
Unknown regions, 3 INCIDENTS <1%
*Due to legal requirements, not all breaches are reported or publicly disclosed.
Regional differences of data may not accurately reflect total data breaches that occur.
Statistics presented are based on the Breach Level Index (breachlevelindex.com)
gemalto
security to be free
SafeNet

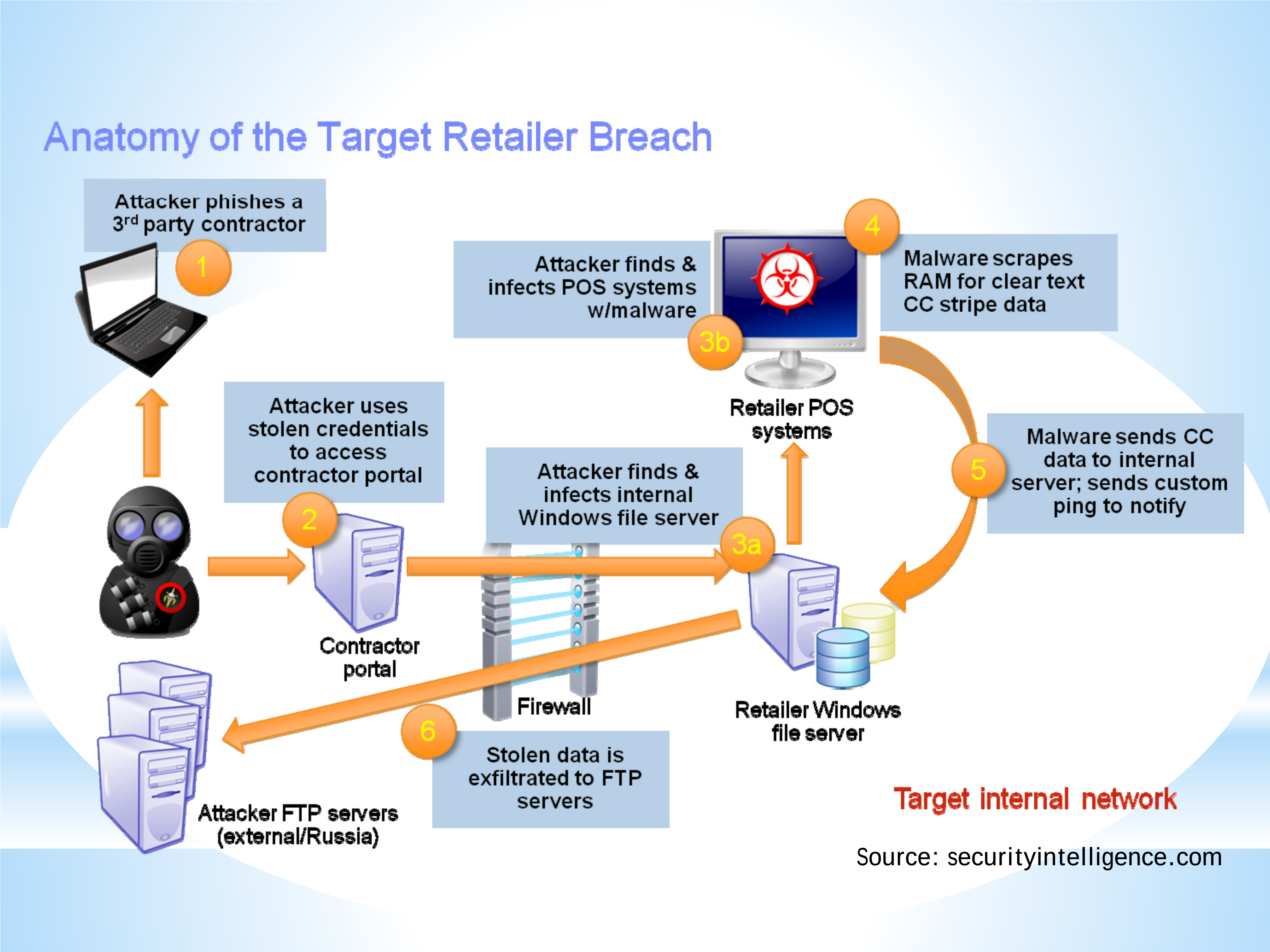
Advanced Persistent Threat (APT):

An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.

Source: NIST SP800-39



Source: secureworks.com


Anatomy of the Target Retailer Breach
Attacker phishes a 3rd party contractor
1
Attacker uses stolen credentials to access contractor portal
2
Contractor portal
Attacker finds & infects internal Windows file server
3a
Firewall
Retailer Windows file server
Attacker finds & infects POS systems w/malware
3b
Retailer POS systems
4
Malware scrapes RAM for clear text CC stripe data
5
Malware sends CC data to internal server; sends custom ping to notify
6
Stolen data is exfiltrated to FTP servers
Attacker FTP servers (external/Russia)
Target internal network
Source: securityintelligence.com

Source: vocativ.com

Lessons Learned?

- No one is too big or too small
- Protection through technology is limited
- A single employee/contractor can unknowingly compromise a multi-billion dollar enterprise
- Individual security is critical

Malware (Viruses, Trojans, Worms, Spyware, Rootkits, Backdoors, Adware, Ransomware):

Short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. In law, malware is sometimes known as a computer contaminant, as in the legal codes of several U.S. states. (wikipedia.com)

Ransomware:

A type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed. (wikipedia.com)

“Honest” Thieves


CryptoLocker
Your personal files are encrypted!
Private key will be destroyed on
9/8/2013
5:52 PM
Time left
56 : 16 : 12
Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 100 USD / 100 EUR / similar amount in another currency.
Click «Next» to select the method of payment and the currency.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Next >>

Reaction to Ransomware?

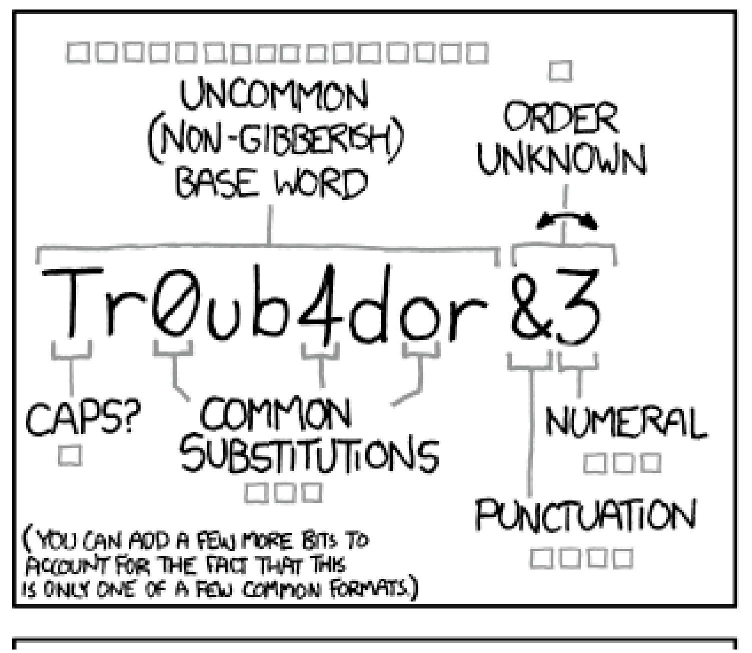
- Policy?
- Legal reporting/responsibilities?
- Police reporting?
- Recovery of data
  - Pay the ransom?
  - Restore from backup?
- Affected system(s)
  - Wipe and return to service?
  - Preserve as evidence?

How do you get malware?

- Phishing Emails
- Compromised/Malicious Ad-servers
- “Drive-by” Downloads
- Infected Email Attachments
- USB Flash Drives
- Compromised/Malicious Wireless Networks
- Infected Applications
- Spam Emails
- Unpatched Systems/Applications
- Direct from Manufacturer

What can you do?

- Always consider security
- Strong passwords
- *Different passwords*
- *Password managers*
- *Dual-factor authentication*
- Keep systems and applications patched and up-to-date
- Private hotspot (avoid public Wi-Fi)
- Be wary of emails, links, attachments
- Be wary of scare tactics – fear is a huge motivator
- Practice safe social media
- Antivirus/anti-malware software
- Ad-blocking
- Teach everyone at home safe computing habits
- *Practice* safe computing habits



Source: xkcd.com

Password1	!QAZ1qaz	Trinity1	Stephanie1	Justice1	Frankie1	Newyork1	Metallica1
Princess1	Patrick1	Chocolate1	Dolphins1	Cowboys1	Elizabeth2	Marissa1	Mercedes1
P@ssw0rd	Welcome1	America1	ABC123abc	Charles1	Douglas1	Liberty1	Mackenzie1
Passw0rd	Iloveyou1	Password01	Spongebob1	Blondie1	Devil666	Lebron23	Kenneth1
Michael1	Bubbles1	Natalie1	Pa$$w0rd	Softball1	Christina1	Jamaica1	Jackson5
Blink182	Chelsea1	Superman1	Forever1	Orlando1	Bradley1	F**kyou1	Genesis1
!QAZ2wsx	ZAQ!2wsx	Scooter1	iydgTvmujl6f	Greenday1	zaq1@WSX	Chester1	Diamonds1
Charlie1	Blessed1	Mustang1	Zachary1	Dominic1	Tigger01	Braxton1	Buttercup1
Anthony1	Richard1	Brittany1	Yankees1	!QAZzaq1	Summer08	August12	Brandon7
1qaz!QAZ	Danielle1	Angel123	Stephen1	abc123ABC	Princess21	z,iyd86I	Whatever1
Brandon1	Raiders1	Jonathan1	Shannon1	Snickers1	Playboy1	l6fkiy9oN	TheSims2
Jordan23	Jackson1	Friends1	John3:16	Patches1	October1	Sweetie1	Summer06
1qaz@WSX	Jesus777	Courtney1	Gerrard8	P@$$w0rd	Katrina1	November1	Starwars1
Jessica1	Jennifer1	Aaliyah1	F**kyou2	Natasha1	Iloveme1	Love4ever	Spiderman1
Jasmine1	Alexander1	Rebecca1	ZAQ!1qaz	Myspace1	Chris123	Ireland1	Soccer11
Michelle1	Ronaldo7	Timothy1	Pebbles1	Monique1	Chicago1	Iloveme2	Skittles1
Diamond1	Heather1	Scotland1	Monster1	Letmein1	Charlotte1	Christine1	Princess01
Babygirl1	Dolphin1	Raymond1	Chicken1	James123	Broncos1	Buttons1	Phoenix1
Iloveyou2	Destiny1	Inuyasha1	zaq1!QAZ	Celtic1888	BabyGirl1	Babyboy1	Pass1234
Matthew1	Brianna1	Tiffany1	Spencer1	Benjamin1	Abigail1	Angel101	Panther1
Rangers1	Trustno1	Pa55w0rd	Savannah1	Baseball1	Tinkerbell1	Vincent1	November11
Pa55word	1qazZAQ!	Nicholas1	Jesusis1	1qazXSW@	Rockstar1	Spartan117	Lindsey1
Iverson3	Precious1	Melissa1	Jeffrey1	Vanessa1	RockYou1	Soccer12	Katherine1
Sunshine1	Freedom1	Isabella1	Houston1	Steelers1	Michelle2	Princess2	JohnCena1
Madison1	Christian1	Summer07	Florida1	Slipknot1	Georgia1	Penguin1	January1
William1	Brooklyn1	Rainbow1	Crystal1	Princess13	Computer1	Password5	Gangsta1
Elizabeth1	!QAZxsw2	Poohbear1	Tristan1	Princess12	Breanna1	Password3	F**koff1
Password123	Password2	Peaches1	Thunder1	Midnight1	Babygurl1	Panthers1	Freddie1
Liverpool1	Football1	Gabriel1	Thumper1	Marines1	Trinity3	Nirvana1	Forever21
Cameron1	ABCabc123	Arsenal1	Special1	M1chelle	Pumpkin1	Nicole12	Death666
Butterfly1	Samantha1	Antonio1	Pr1ncess	Lampard8	Princess7	Nichole1	Chopper1
Beautiful1	Charmed1	Victoria1	Password12	Jesus123	Preston1	Molly123	Arianna1

Source: RockYou leak, 2009

Most Common & Worst Passwords of 2014

Rank	Password	Change from 2013
1	123456	Unchanged
2	password	Unchanged
3	12345	Up 17
4	12345678	Down 1
5	qwerty	Down 1
6	123456789	Unchanged
7	1234	Up 9
8	baseball	New
9	dragon	New
10	football	New
11	1234567	Down 4
12	monkey	Up 5
13	letmein	Up 1
14	abc123	Down 9
15	111111	Down 8
16	mustang	New
17	access	New
18	shadow	Unchanged
19	master	New
20	michael	New
21	superman	New
22	696969	New
23	123123	Down 12
24	batman	New
25	trustno1	Down 1

via Splashdata analysis

Analysis of ~3.3 million leaked passwords

Even with Target, Home Depot, and others in the news, people still use weak and common passwords

Password Guidelines:

Longer = Better

Use all 4 common character types:

- Uppercase
- Lowercase
- Numbers
- Special Characters (!@#$%....)

Use character substitutions

Don’t use dictionary words

Don’t use patterns/keyboard layout

Tr0ub4dor&3

correct horse battery staple

Oh, I ate87 tacos@Chuy’s

Data Loss Prevention (DLP):

Data loss prevention is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.
(techtarget.com)

- Policy
- Computer Usage Agreements – Employees/consultants
- Technology
  - Scan data in transit
  - Decrypt all data and analyze

Decrypting Data – The Conundrum

Just because you can, should you?

- Discoverable?
- Data Retention?
- All or One or None?
- Negative Perception – Big Brother is Watching
- Employee Trust and Morale

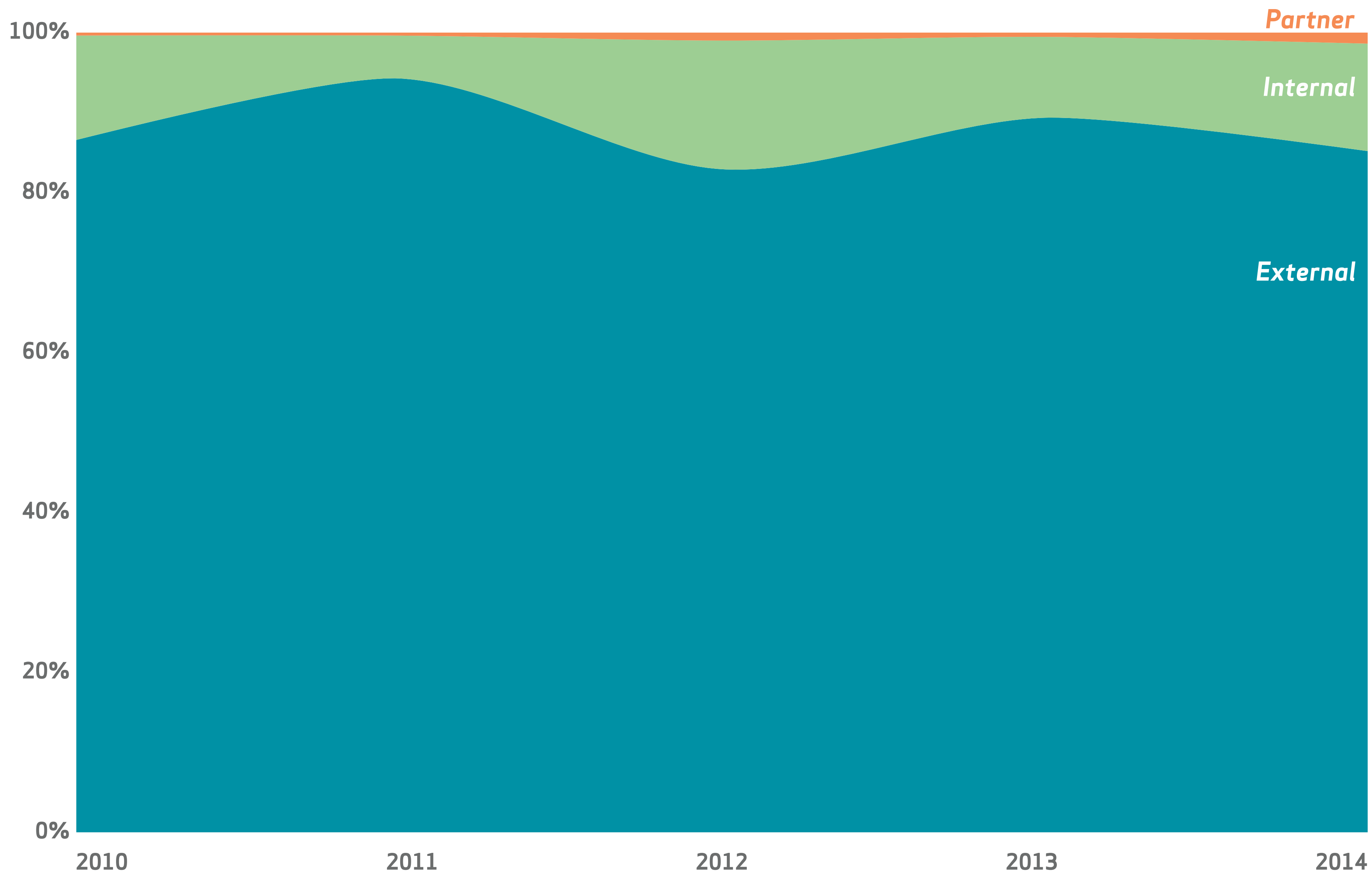
Thank you!

Protecting Data and Cyber Security

PREPARING FOR ADVANCED CYBER SECURITY THREATS

PREPARED FOR NAPPA ON JUNE 25, 2015 IN AUSTIN, TX — BY JOSH ABRAHAM (@JABRA)

Breaches by Threat Actors



Though the number of breaches per threat actor changes rather dramatically each year, the overall proportion attributed to external, internal, and partner actors stays roughly the same.

Actor categories over time by percent of actors

Source: Verizon Data Breach Report (2015

Disclosures by Incident Type (Financial Services)

CRIMEWARE	CYBER-ESPIONAGE	DENIAL OF SERVICE
36%	–	–
LOST AND STOLEN ASSETS	**MISCELLANEOUS ERRORS**	**PAYMENT CARD SKIMMERS**
2%	7%	14%
POINT OF SALE	**PRIVILEGE MISUSE**	**WEB APPLICATIONS**
–	11%	31%

Frequency of data disclosures by incident patterns for financial services industry

Crimeware and Web applications rank high for **Financial services**

Source: Verizon Data Breach Report (2015

Variety of Malware within Crimeware Pattern

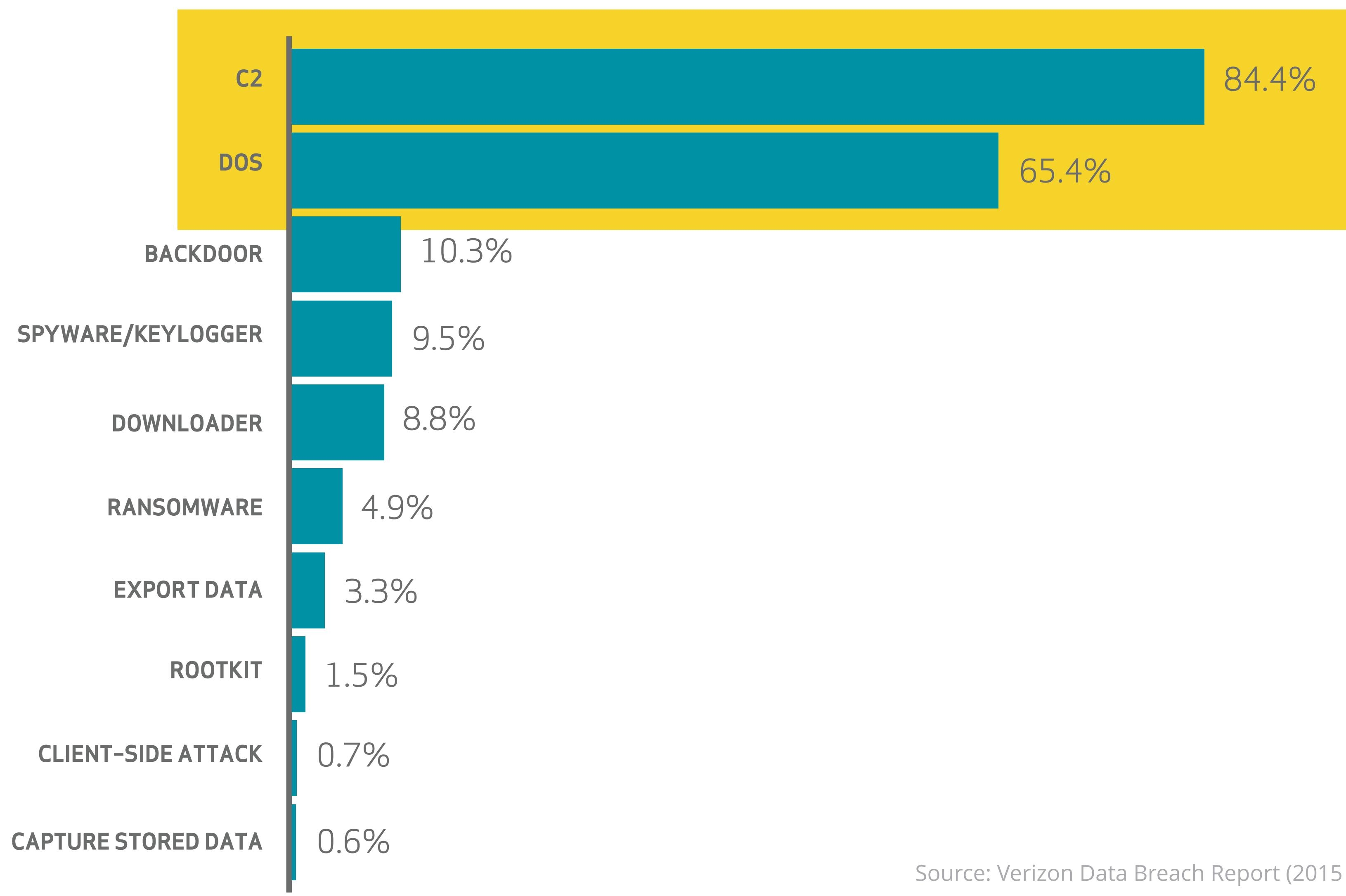
CRIMEWARE

36%

WEB APPLICATIONS

31%

Crimeware represents malware infections within organizations that are not associated with more specialized classification patterns.



Source: Verizon Data Breach Report (2015

Variety of Data Compromised within Crimeware

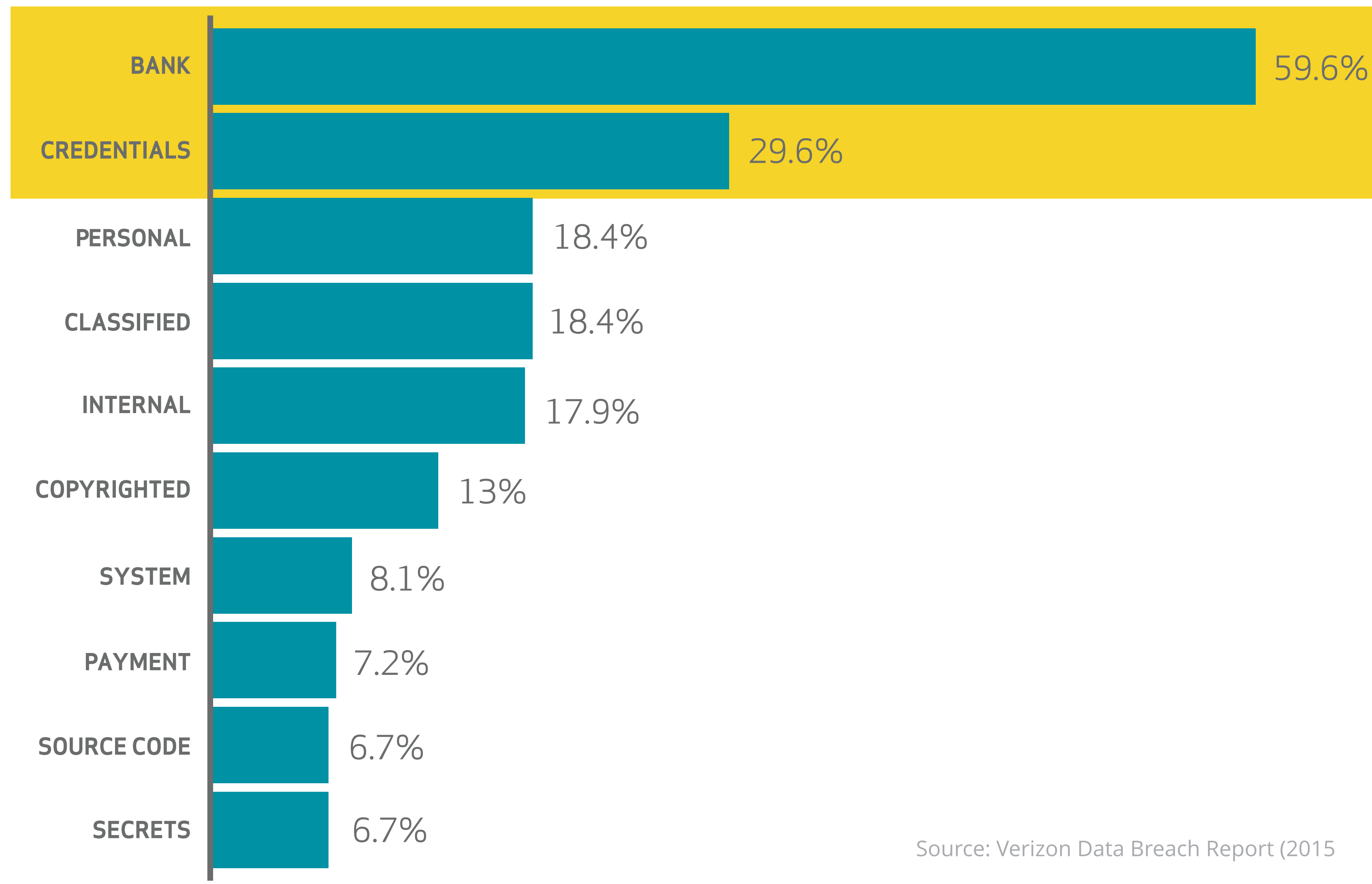
CRIMEWARE

36%

WEB APPLICATIONS

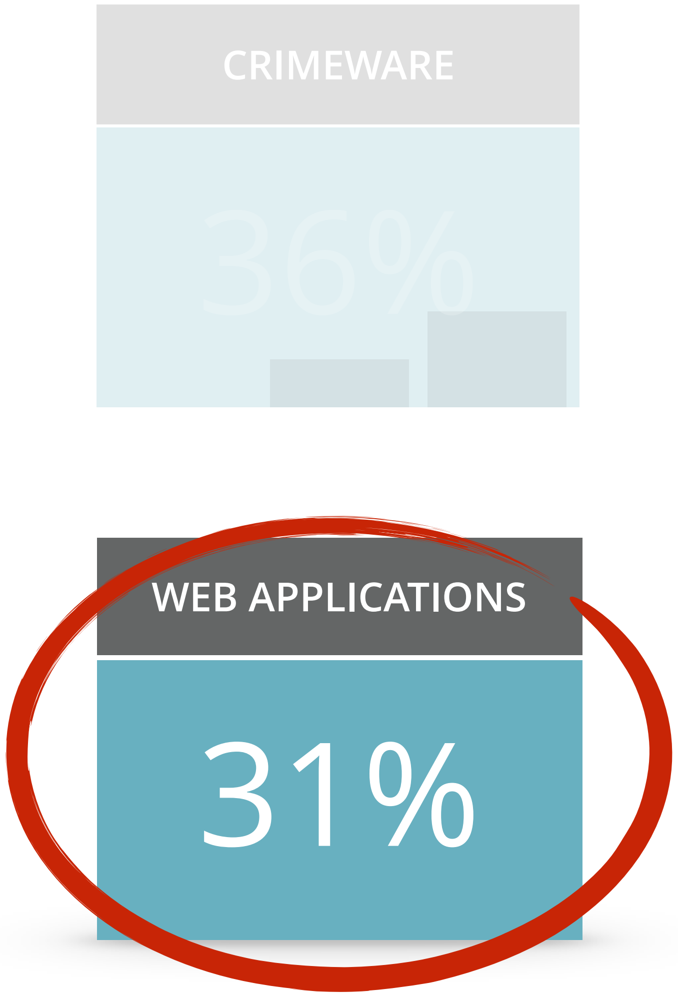
31%

When there is confirmed data breaches, bank records and credentials traded places for the top spot

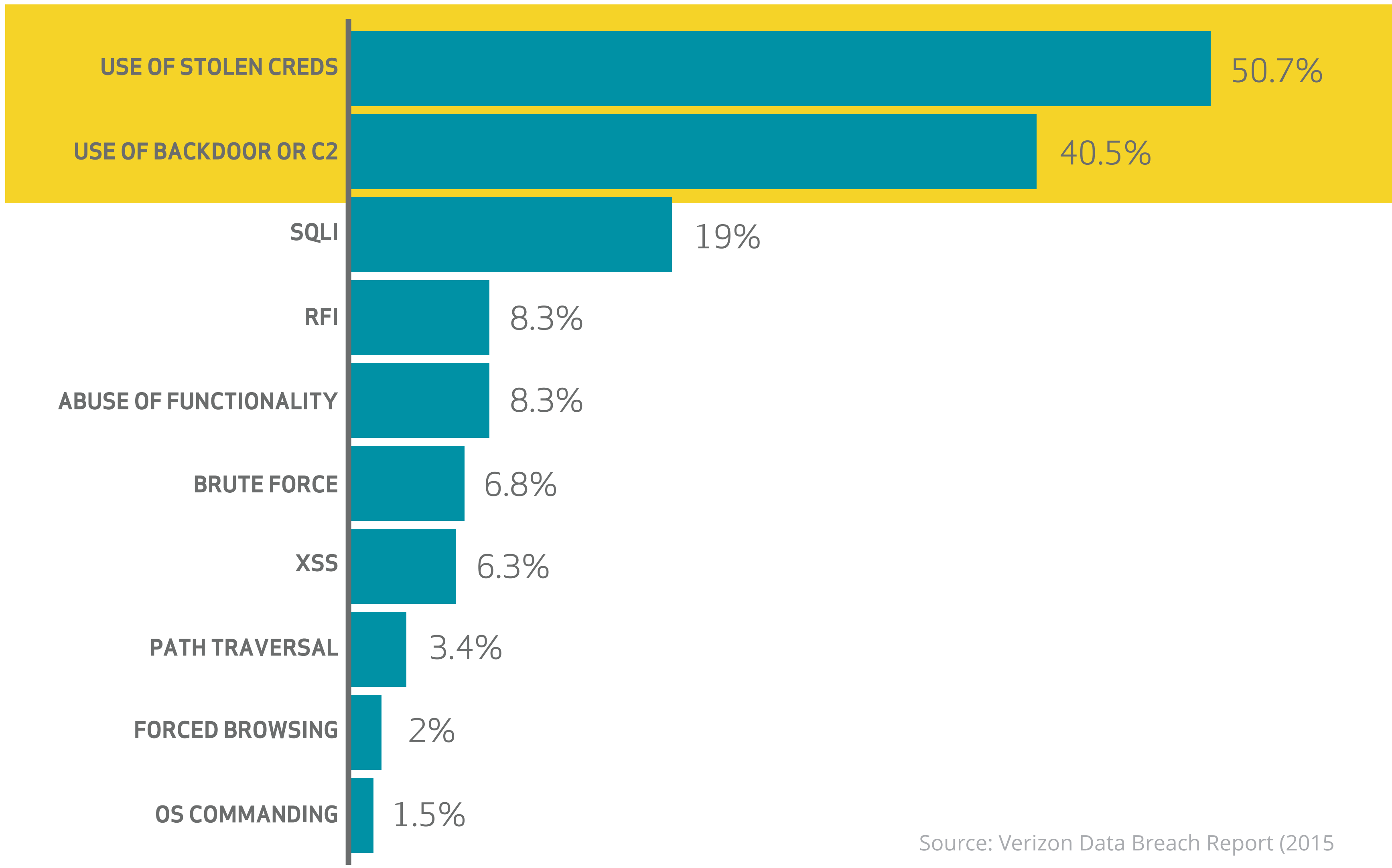


Source: Verizon Data Breach Report (2015

Variety of Hacking Actions within Web App Attacks

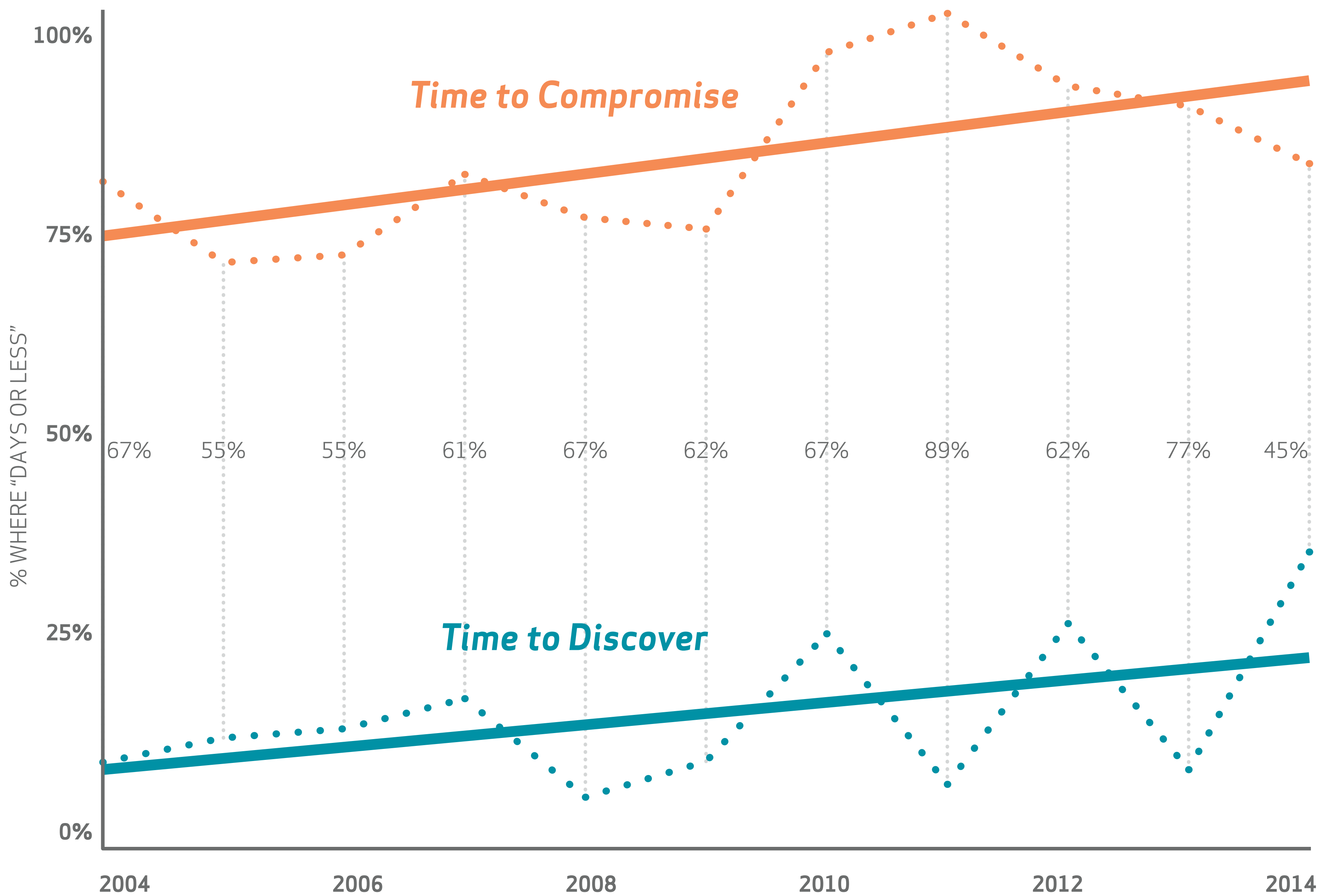


This year, organized crime became the most frequently seen threat actor for Web App Attacks.



Source: Verizon Data Breach Report (2015

Time-of-Compromise vs Time-of-Detection



Unfortunately, the proportion of breaches discovered within days still falls well below that of time to compromise.

The defender-detection deficit

Source: Verizon Data Breach Report (2015

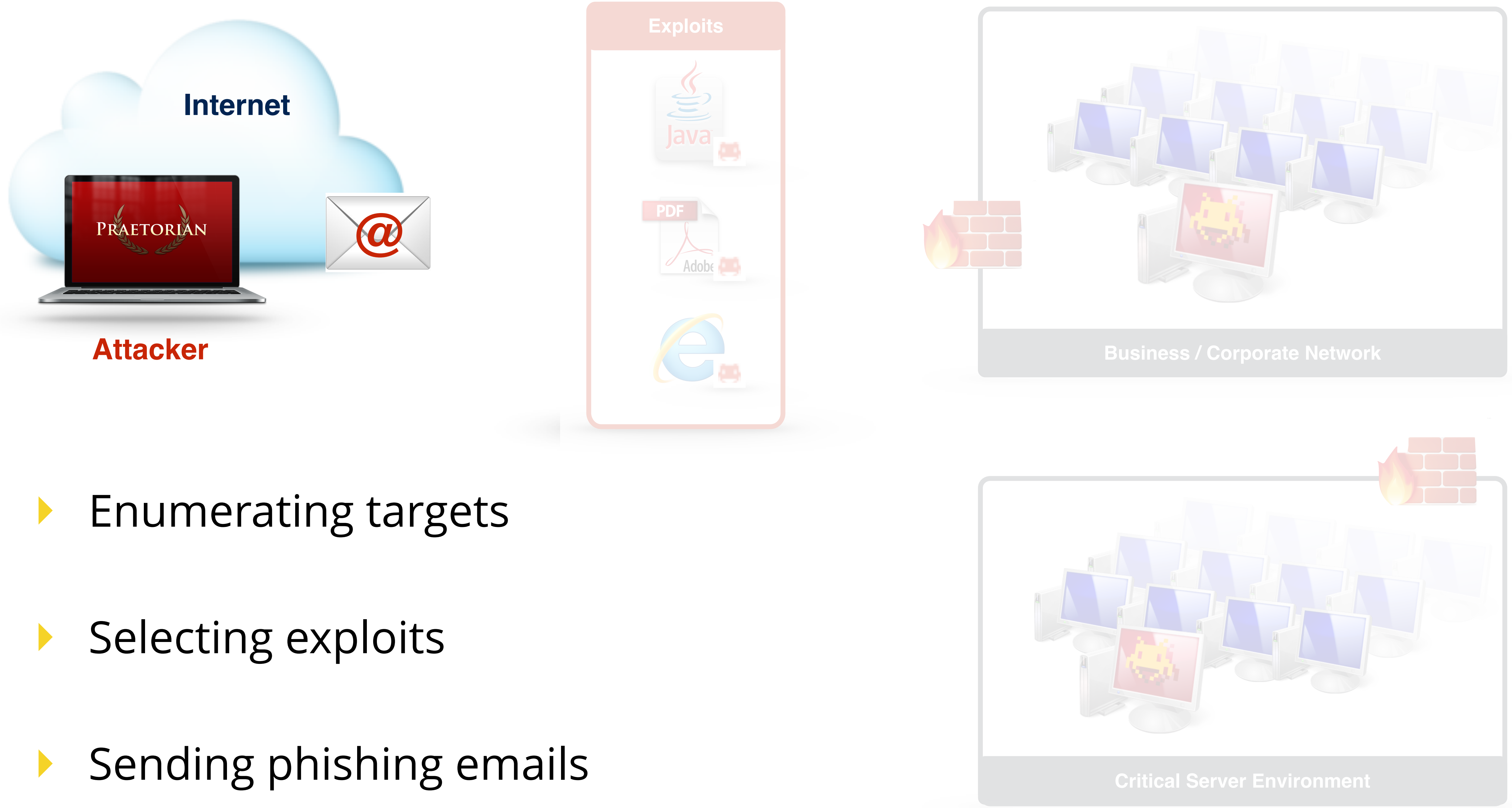
Phishing / Social Engineering

You are the weakest link

The reality is that you don't have time on your side when it comes to detecting and reacting to phishing events.

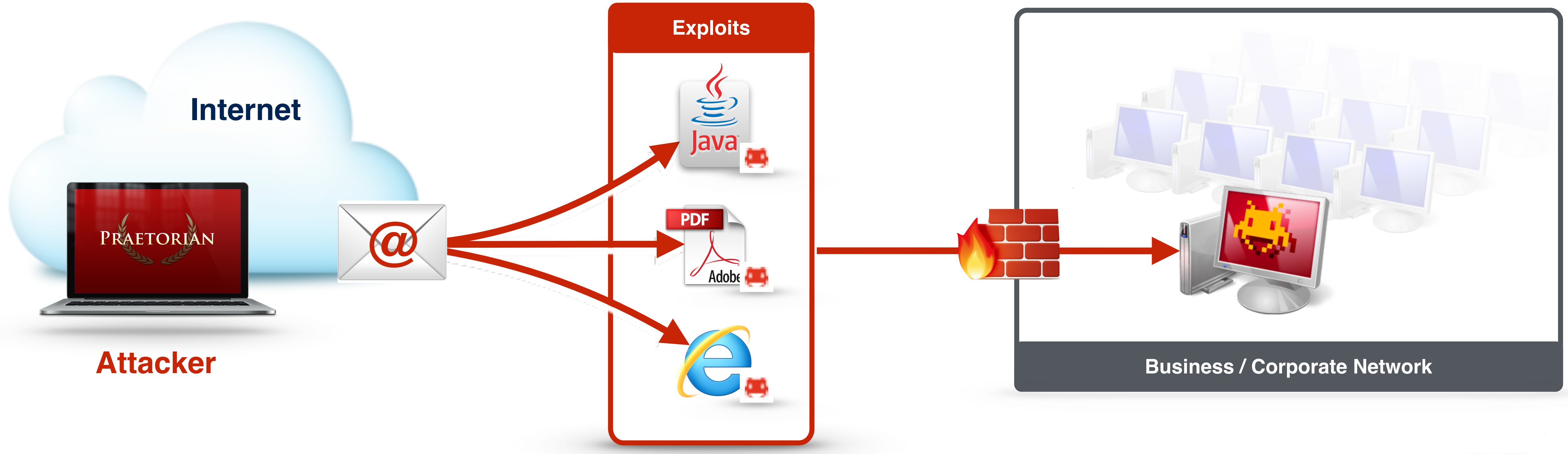
Nearly 50% open e-mails and click on phishing links within the first hour.

Phishing Attacks



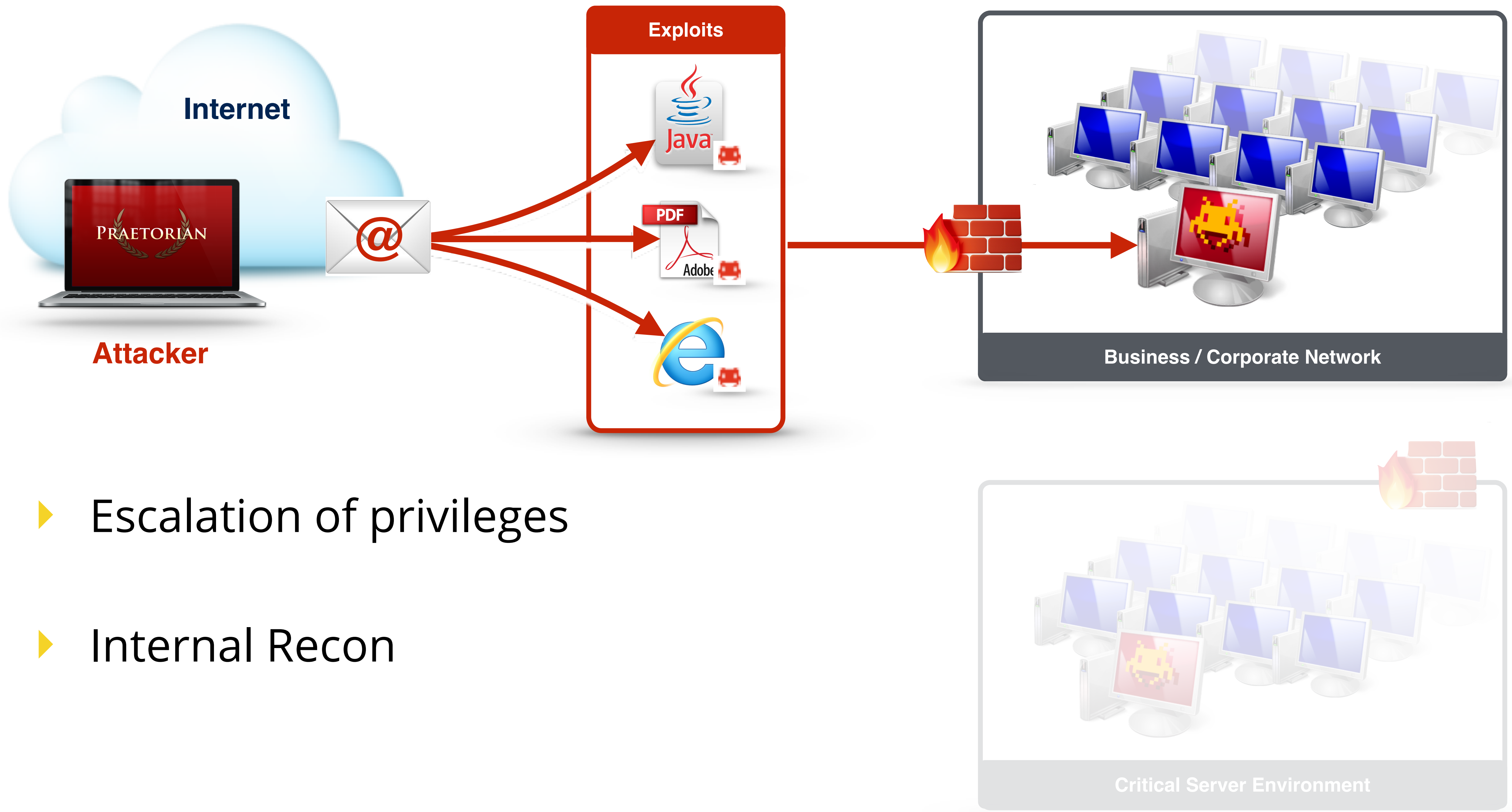
- Enumerating targets
- Selecting exploits
- Sending phishing emails

Initial Compromise



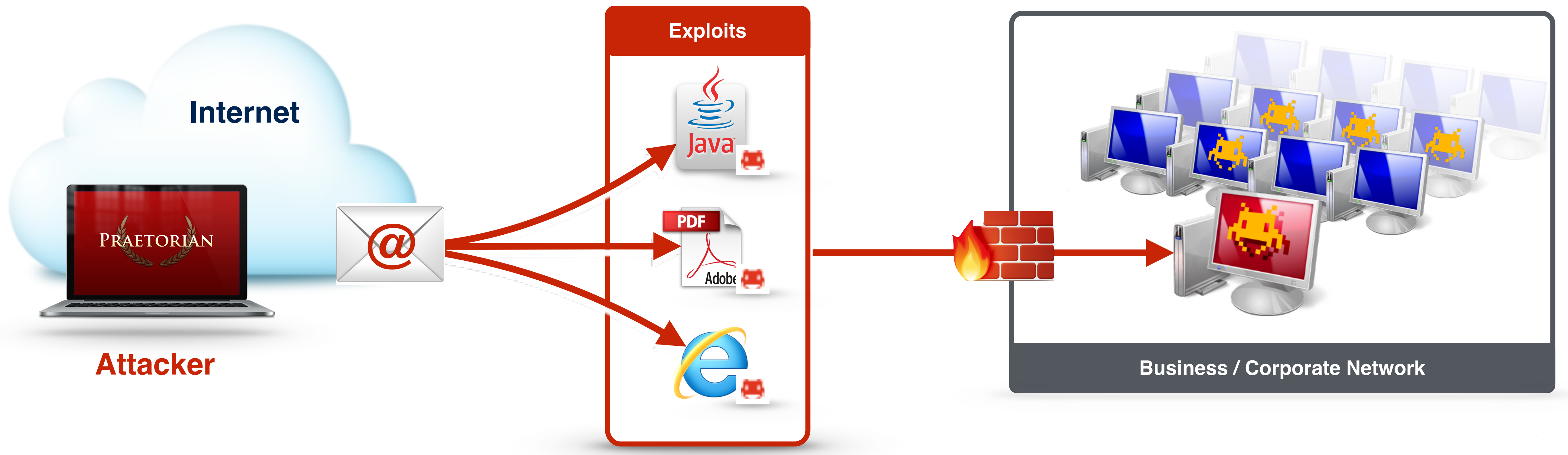
- Victim runs Java Applet
- Victim opens malicious PDF
- Victim clicks malicious link

After the Initial Compromise



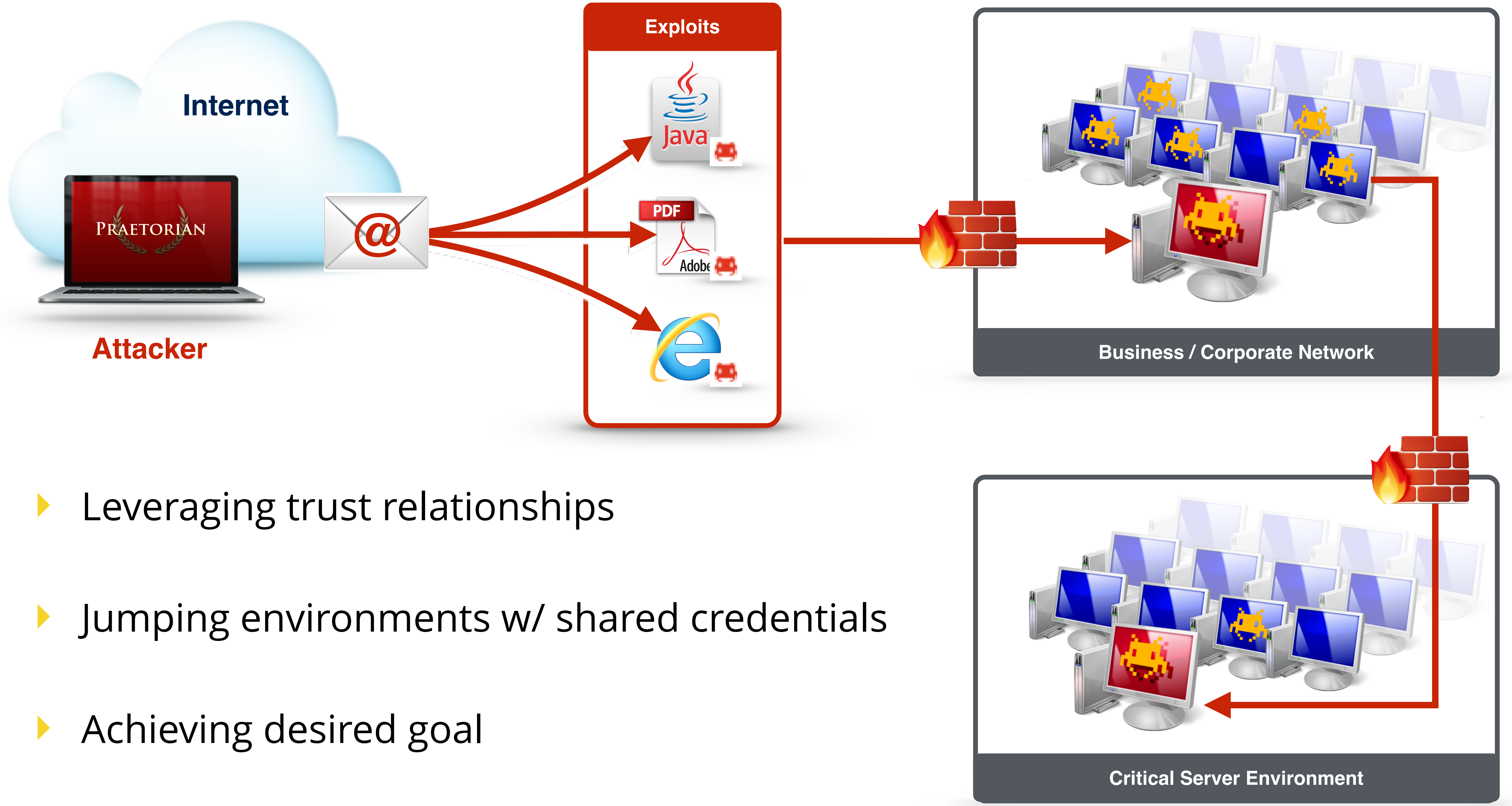
- Escalation of privileges
- Internal Recon

Lateral Movement



- Stealing Credentials / Keys
- Impersonation Based Attacks
- Leveraging design weaknesses

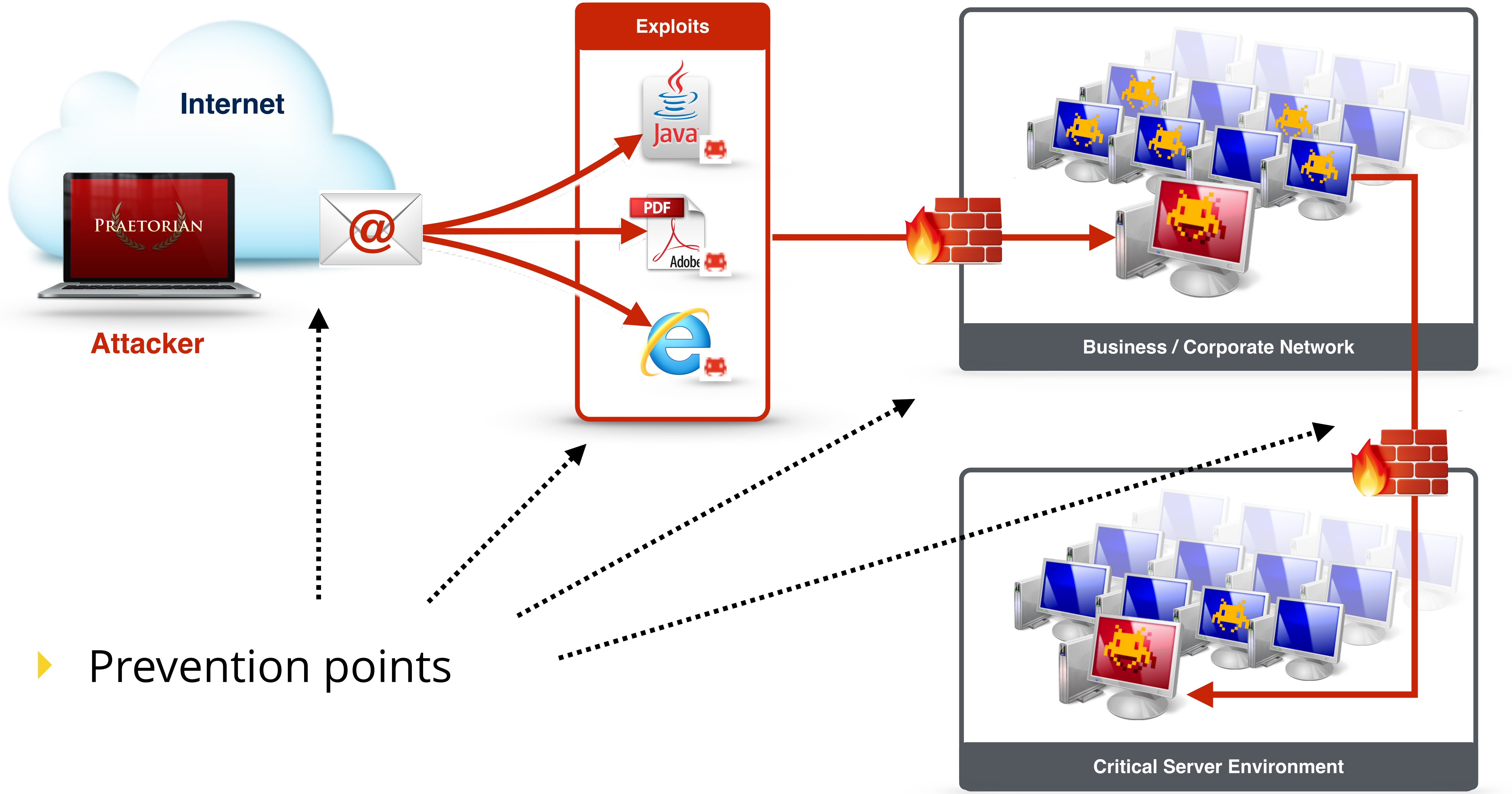
Lateral Movement



- Leveraging trust relationships
- Jumping environments w/ shared credentials
- Achieving desired goal

Praetorian

Complete Compromise



- Prevention points

Prevention Efforts & Response Capabilities

How does your organization close the **Security Gap?**

Q/A

Josh Abraham (@jabra)

VP of Professional Services

josh.abraham@praetorian.com

PRAETORIAN

The Security Experts

INFORMATION SECURITY ASSESSMENT AND ADVISORY

NETWORK

APPLICATION

MOBILE

CLOUD

IOT