Crowe Horwath.

Smart decisions. Lasting value.™

Cybersecurity Trends and Threats

NAW Roundtable

November 2, 2017

Michael Lucas

Agenda

- Introductions
- Think like an Attacker
- Cybersecurity Trends
- Securing Yourself
- Questions

Michael Lucas
Senior Manager, Cybersecurity
Michael.Lucas@crowehorwath.com
Cell: +1(317) 850-3651

Think Like an Attacker!

Password Policy for Company X:

Length: 8 characters

Complexity Required: Three of the four (A, a, 1, !)

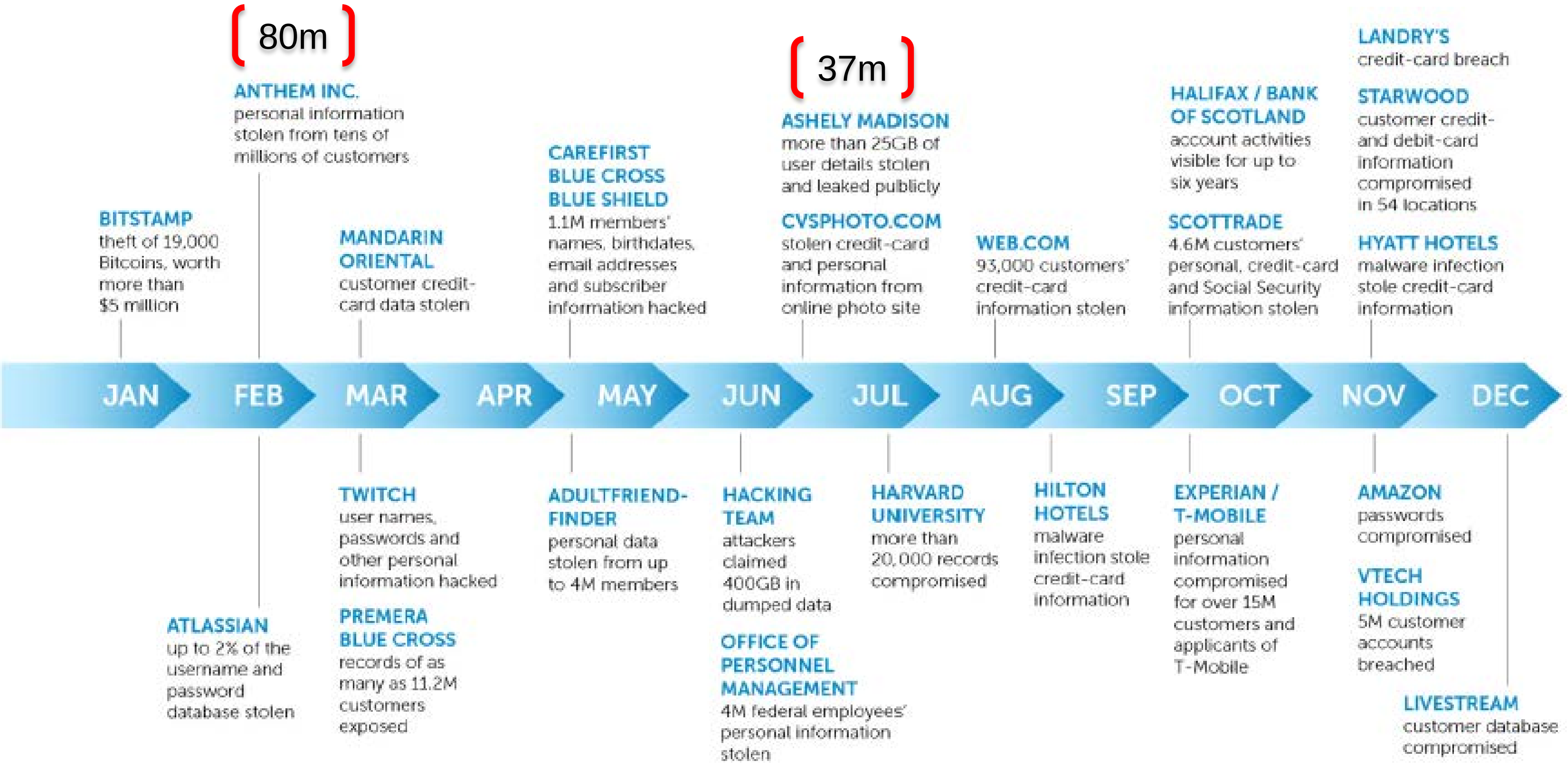
Lockout: 3 Attempts

Lockout Duration: Forever

QUESTION: Given the above password complexity is enabled on the system, what be would ***your first guess*** for user account passwords?

Cybersecurity Primer

Breaches By The Numbers



BITSTAMP
theft of 19,000 Bitcoins, worth more than $5 million

80m

ANTHEM INC.
personal information stolen from tens of millions of customers

ATLASSIAN
up to 2% of the username and password database stolen

MANDARIN ORIENTAL
customer credit-card data stolen

TWITCH
user names, passwords and other personal information hacked

PREMERA BLUE CROSS
records of as many as 11.2M customers exposed

CAREFIRST BLUE CROSS BLUE SHIELD
1.1M members' names, birthdates, email addresses and subscriber information hacked

ADULTFRIEND-FINDER
personal data stolen from up to 4M members

HACKING TEAM
attackers claimed 400GB in dumped data

OFFICE OF PERSONNEL MANAGEMENT
4M federal employees' personal information stolen

37m

ASHELY MADISON
more than 25GB of user details stolen and leaked publicly

CVSPHOTO.COM
stolen credit-card and personal information from online photo site

HARVARD UNIVERSITY
more than 20,000 records compromised

WEB.COM
93,000 customers' credit-card information stolen

HILTON HOTELS
malware infection stole credit-card information

HALIFAX / BANK OF SCOTLAND
account activities visible for up to six years

SCOTTRADE
4.6M customers' personal, credit-card and Social Security information stolen

EXPERIAN / T-MOBILE
personal information compromised for over 15M customers and applicants of T-Mobile

LANDRY'S
credit-card breach

STARWOOD
customer credit- and debit-card information compromised in 54 locations

HYATT HOTELS
malware infection stole credit-card information

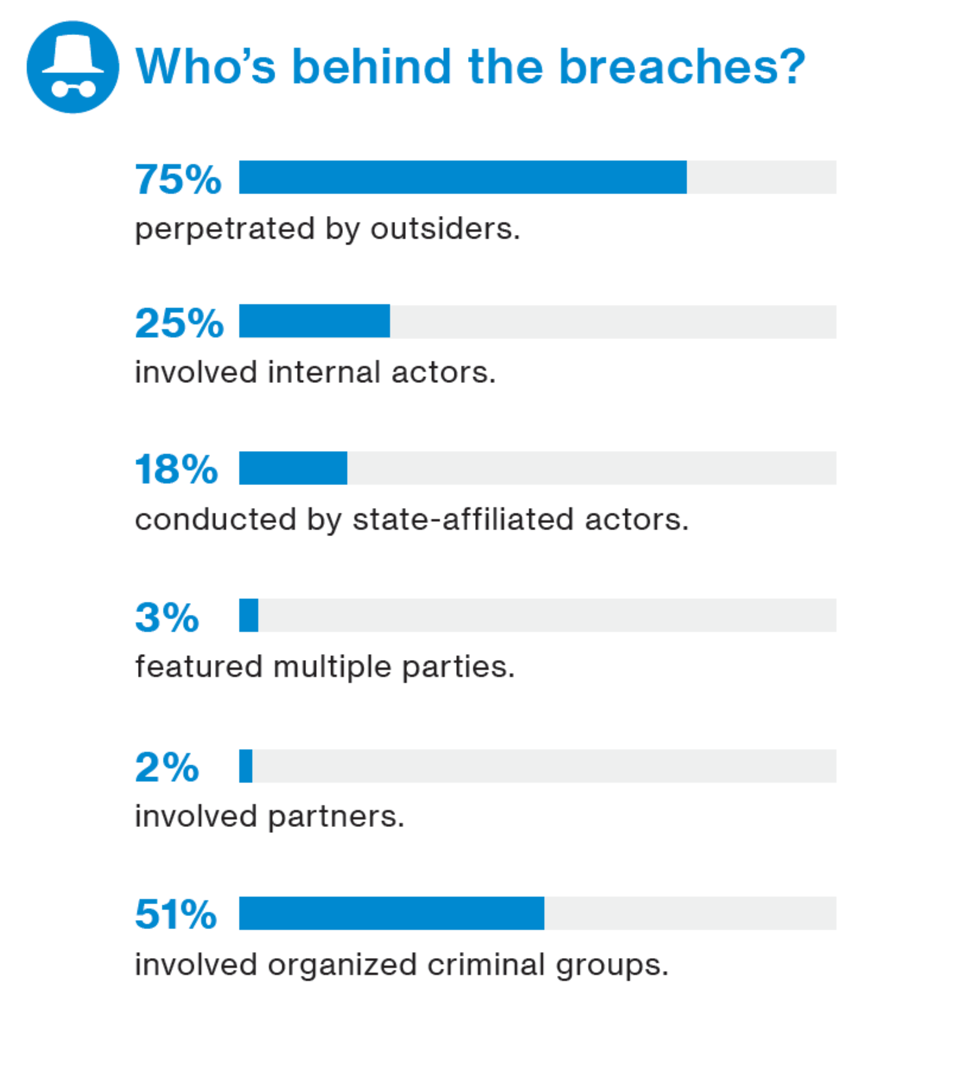
AMAZON
passwords compromised

VTECH HOLDINGS
5M customer accounts breached

LIVESTREAM
customer database compromised

[1] *dell security 2016 threat report:* http://dell.to/1QeaJ4X

Tactics and Adversaries



Who’s behind the breaches?

75%
perpetrated by outsiders.

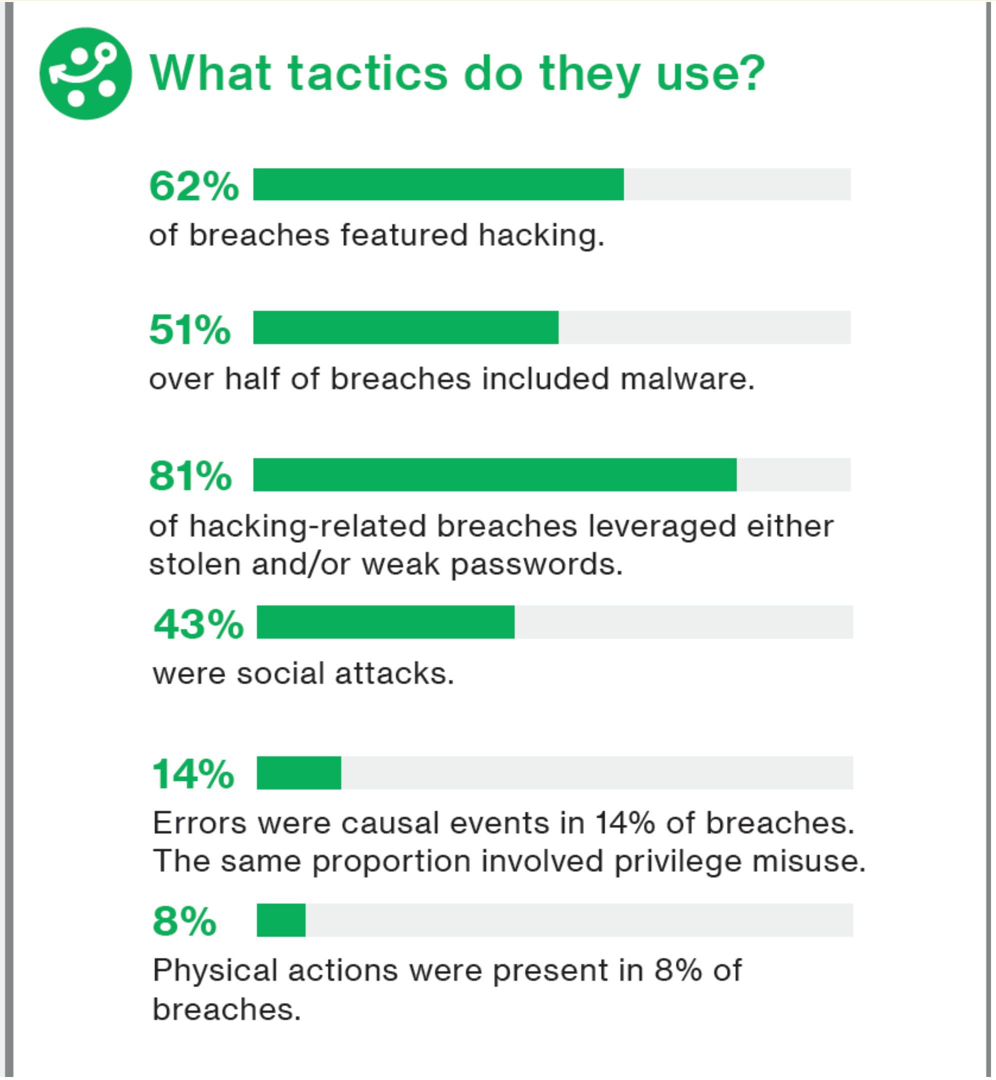
25%
involved internal actors.

18%
conducted by state-affiliated actors.

3%
featured multiple parties.

2%
involved partners.

51%
involved organized criminal groups.



What tactics do they use?

62%
of breaches featured hacking.

51%
over half of breaches included malware.

81%
of hacking-related breaches leveraged either stolen and/or weak passwords.

43%
were social attacks.

14%
Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8%
Physical actions were present in 8% of breaches.

Who is targeted?

Who are the victims?

24%

of breaches affected financial organizations.

15%

of breaches involved healthcare organizations.

12%

Public sector entities were the third most prevalent breach victim at 12%.

15%

Retail and Accommodation combined to account for 15% of breaches.

What else is common?

66%

of malware was installed via malicious email attachments.

73%

of breaches were financially motivated.

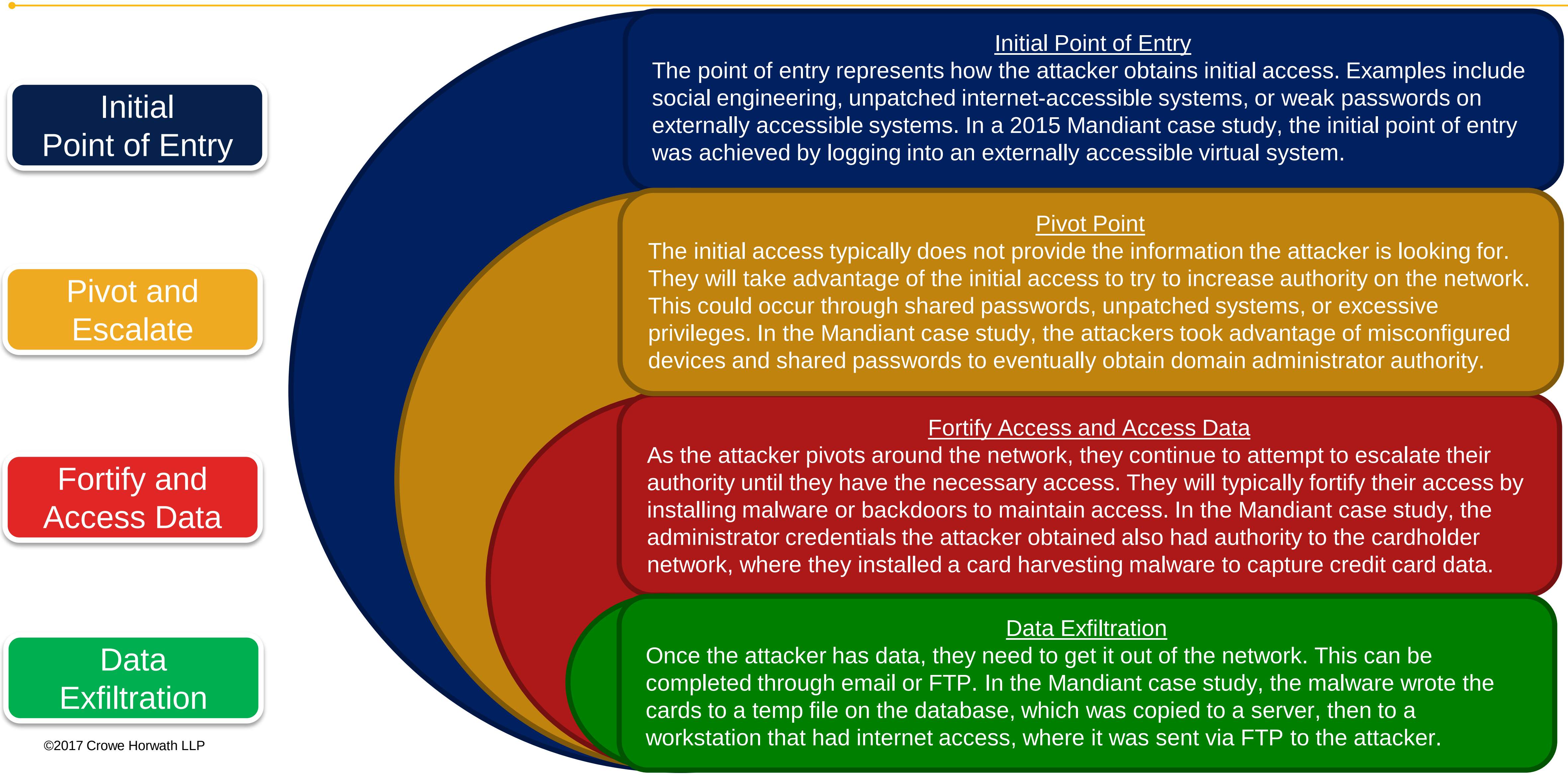
21%

of breaches were related to espionage.

27%

of breaches were discovered by third parties.

How do breaches actually happen?



Initial Point of Entry

Pivot and Escalate

Fortify and Access Data

Data Exfiltration

Initial Point of Entry

The point of entry represents how the attacker obtains initial access. Examples include social engineering, unpatched internet-accessible systems, or weak passwords on externally accessible systems. In a 2015 Mandiant case study, the initial point of entry was achieved by logging into an externally accessible virtual system.

Pivot Point

The initial access typically does not provide the information the attacker is looking for. They will take advantage of the initial access to try to increase authority on the network. This could occur through shared passwords, unpatched systems, or excessive privileges. In the Mandiant case study, the attackers took advantage of misconfigured devices and shared passwords to eventually obtain domain administrator authority.

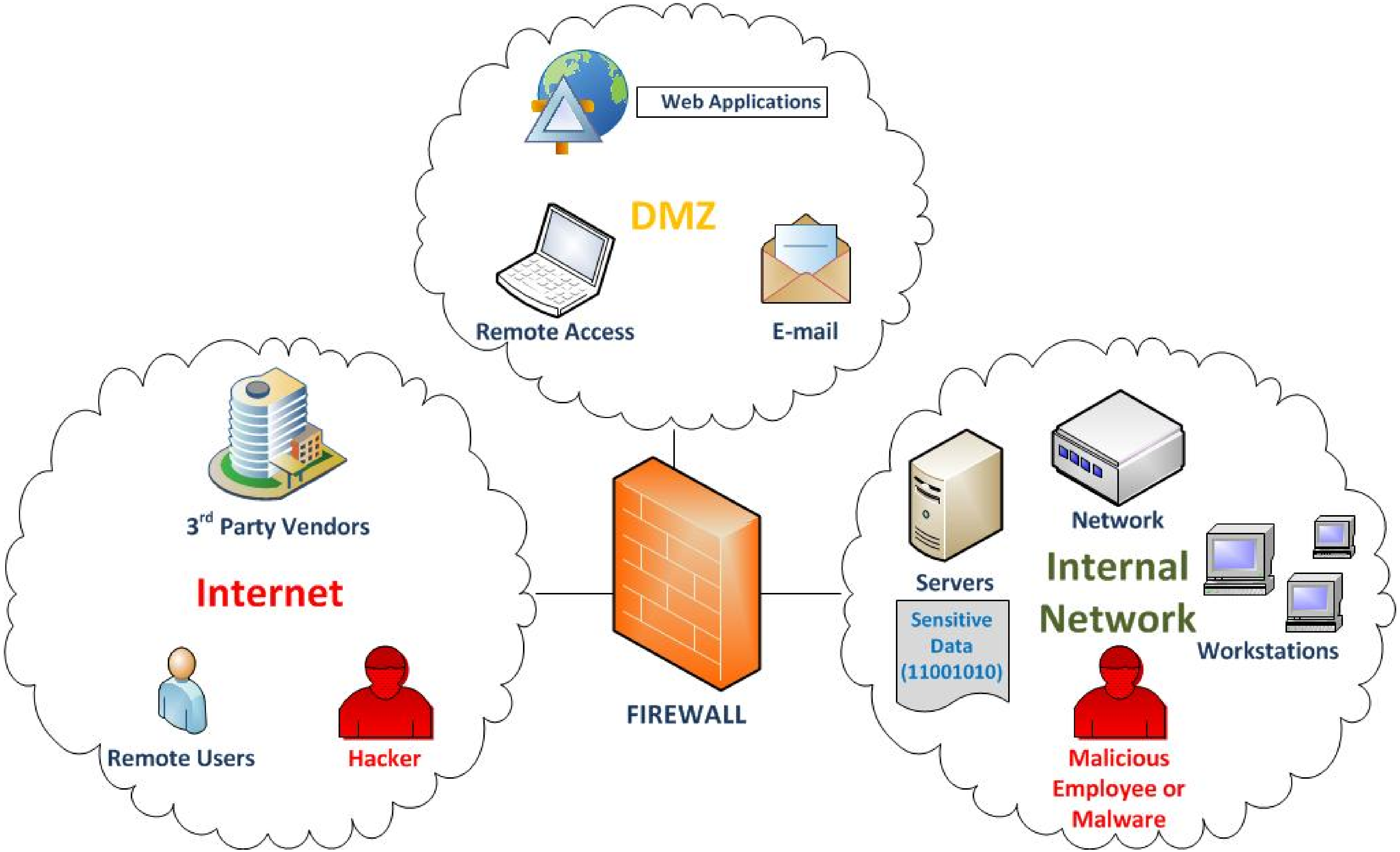
Fortify Access and Access Data

As the attacker pivots around the network, they continue to attempt to escalate their authority until they have the necessary access. They will typically fortify their access by installing malware or backdoors to maintain access. In the Mandiant case study, the administrator credentials the attacker obtained also had authority to the cardholder network, where they installed a card harvesting malware to capture credit card data.

Data Exfiltration

Once the attacker has data, they need to get it out of the network. This can be completed through email or FTP. In the Mandiant case study, the malware wrote the cards to a temp file on the database, which was copied to a server, then to a workstation that had internet access, where it was sent via FTP to the attacker.

Infrastructure Definitions



Cybersecurity Trends

Ransomware [defined]

Per the FBI Cyber Division

✓Ransomware is a form of malware that targets both human and technical weaknesses in organizations and individual networks in an effort to deny the availability of critical data and systems.

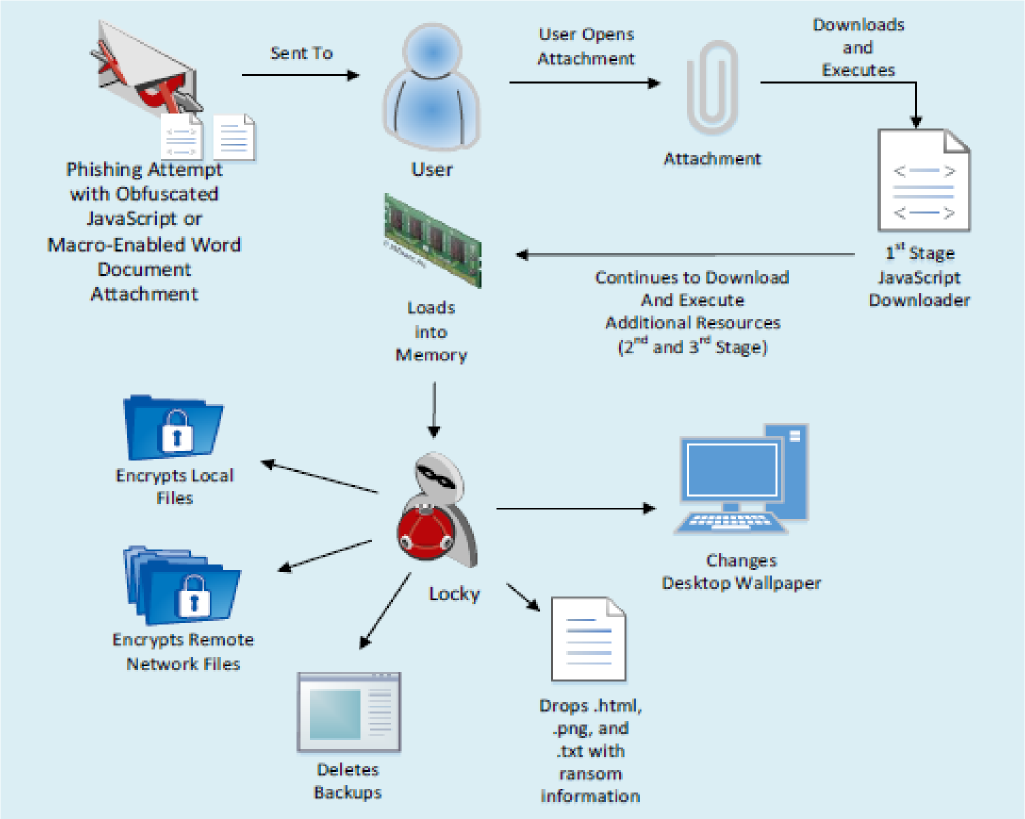
- Evolution
  - ✓First reported instances of ransomware – 1989, using floppy disks!
  - ✓Research on the subject matter first produced in 1996
  - ✓Modern-day ransomware began in 2005
  - ✓First “mass-deployed ransomware” in 2012

Cyber extortion on pace to be **$1billion/year crime in 2016,** per FBI
http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/

Source: Cisco Talos Blog, “Ransomware: Past, Present, and Future,” April 11, 2016,
http://blog.talosintel.com/2016/04/ransomware.html#ch2

Ransomware [attack flow]

- ✓Primary attack vector: social engineering
- ✓Takeaway: Results are different, but attack vectors and recommendations are ***not***
- ✓Moment to pause: What would the **impact** to your organization be? Loss of:
  - ✓Files
  - ✓Workstation(s)
  - ✓Servers



Phishing Attempt with Obfuscated JavaScript or Macro-Enabled Word Document Attachment
Sent To
User
User Opens Attachment
Attachment
Downloads and Executes
1st Stage JavaScript Downloader
Continues to Download And Execute Additional Resources (2nd and 3rd Stage)
Loads into Memory
Locky
Encrypts Local Files
Encrypts Remote Network Files
Deletes Backups
Drops .html, .png, and .txt with ransom information
Changes Desktop Wallpaper

Source: "Ransomware: Locky" (version 2), Information Assurance Directorate at the National Security Agency, https://www.iad.gov/iad/library/ia-guidance/tech-briefs/ransomeware-locky.cfm – Used with permission

Ransomware [preparedness]

Tactically, what should we be reviewing?

✓**Email content filtering:** What is able to be delivered to employees?

✓**Security awareness:** How well are employees trained?

✓**Endpoint protection:** Is there a layered approach?

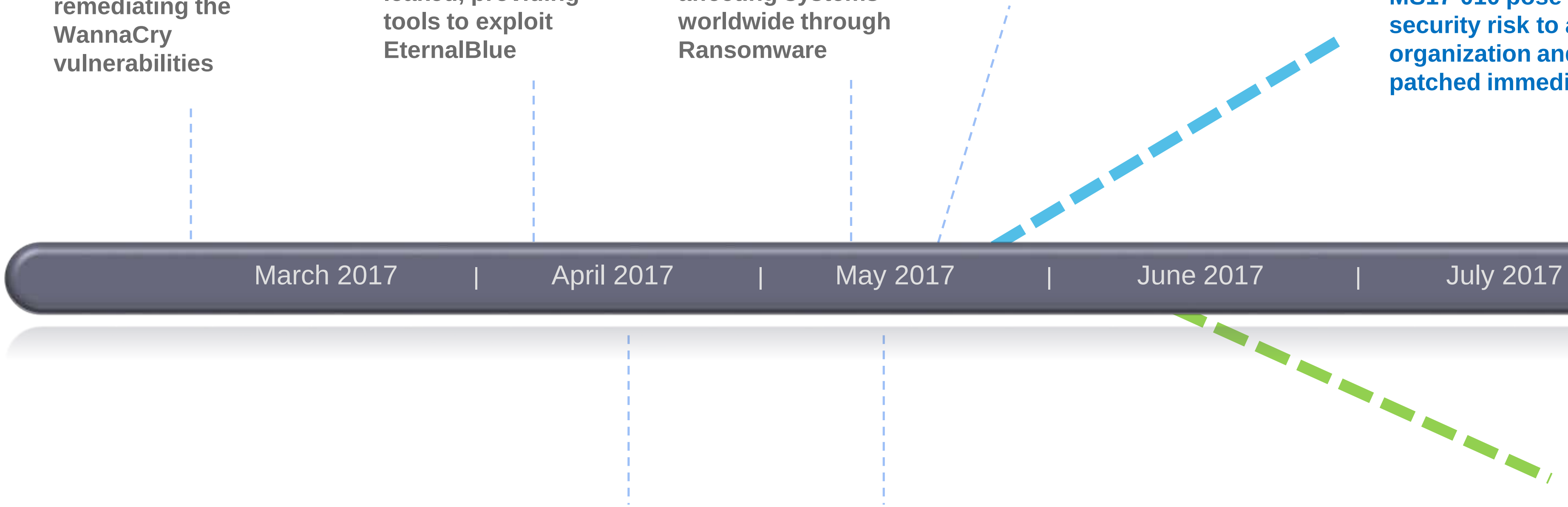
✓**Propagation:** Are we limiting the avenues for privilege escalation, including local administrator? Share permissions?

✓**Data backups:** Have procedures been tested?

✓**Data exfiltration:** What channels of communication are available outbound?

✓**Incident response**: Can we respond in a timely manner with the right skills?

WannaCry Timeline of Events



March 14, 2017: Microsoft release patch MS17-010, remediating the WannaCry vulnerabilities

April 14, 2017: NSA tools were leaked, providing tools to exploit EternalBlue

May 12, 2017: WannaCry began affecting systems worldwide through Ransomware

May: Multiple corporations and nations across the globe are still being affected by WannaCry

Moving Forward: All systems vulnerable to MS17-010 pose a major security risk to any organization and should be patched immediately.

April 21, 2017: Thousands of devices had started to be compromised by NSA Tools.

May 13, 2017: WannaCry propagation halted by a domain registration kill switch

It is expected that additional attacks will occur related to the April 14th exposure.

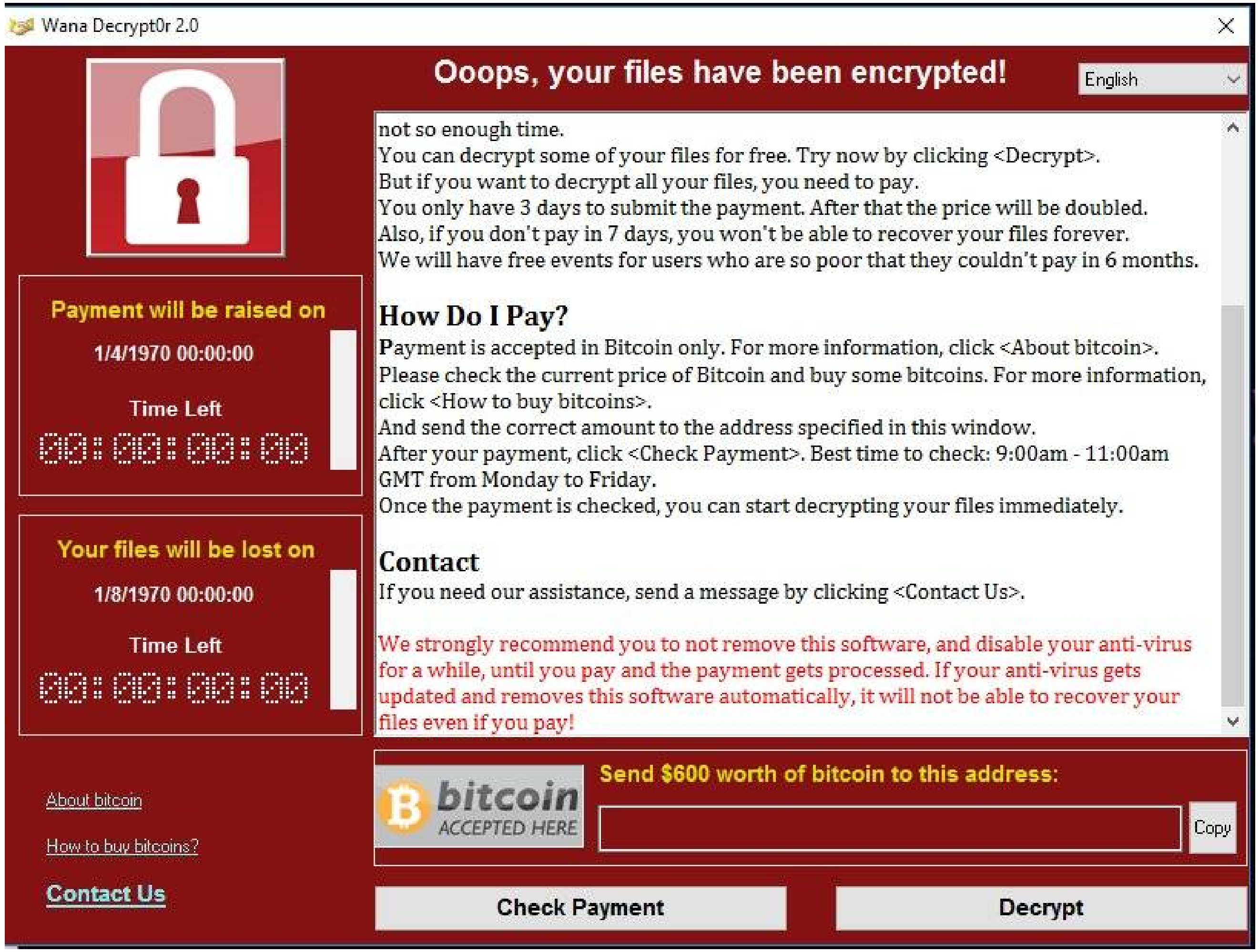
WannaCry Ransomware Infection

What Happens:

- Average ask is $300 US
- 3 Day Timer
- Cost Escalation and Lock

Remediation:

- Make Payment and Cross Fingers
- Wipe and Restore



Ooops, your files have been encrypted!

not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.
Once the payment is checked, you can start decrypting your files immediately.

Contact

If you need our assistance, send a message by clicking <Contact Us>.

We strongly recommend you to not remove this software, and disable your anti-virus for a while, until you pay and the payment gets processed. If your anti-virus gets updated and removes this software automatically, it will not be able to recover your files even if you pay!

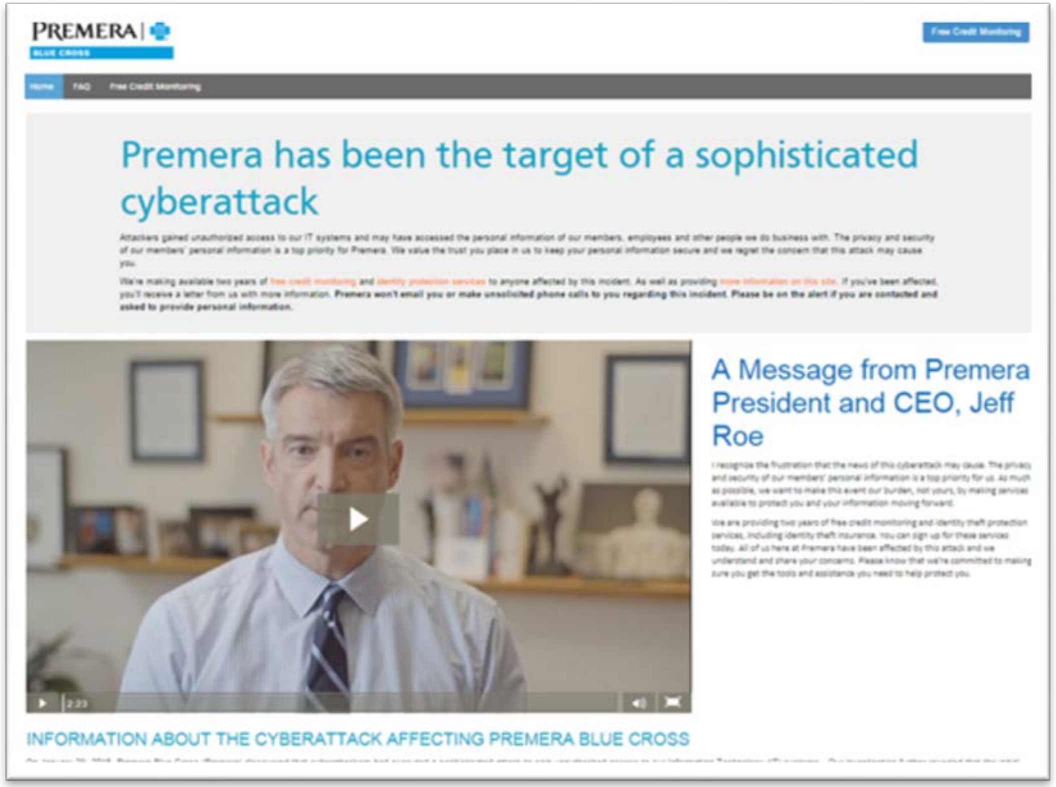
Send $600 worth of bitcoin to this address:

Be Prepared – Incident Response Planning

27% of organizations don’t have a breach response plan or team in place

37% have not reviewed or updated their plan since
 it was created

✓What will I do?
✓What are the laws?
✓What will my regulator say?
✓How much will my customers ask?
✓Who will I call?
✓How do I stop it?



Premera has been the target of a sophisticated cyberattack

Attackers gained unauthorized access to our IT systems and may have accessed the personal information of our members, employees and other people we do business with. The privacy and security of our members' personal information is a top priority for Premera. We value the trust you place in us to keep your personal information secure and we regret the concern that this attack may cause you.

We're making available two years of free credit monitoring and identity protection services to anyone affected by this incident. As well as providing more information on this site. If you've been affected, you'll receive a letter from us with more information. **Premera won't email you or make unsolicited phone calls to you regarding this incident. Please be on the alert if you are contacted and asked to provide personal information.**

A Message from Premera President and CEO, Jeff Roe

I recognize the frustration that the news of this cyberattack may cause. The privacy and security of our members' personal information is a top priority for us. As much as possible, we want to make this event our burden, not yours, by making services available to protect you and your information moving forward.

We are providing two years of free credit monitoring and identity theft protection services, including identity theft insurance. You can sign up for these services today. All of us here at Premera have been affected by this attack and we understand and share your concerns. Please know that we're committed to making sure you get the tools and assistance you need to help protect you.

INFORMATION ABOUT THE CYBERATTACK AFFECTING PREMERA BLUE CROSS

Spear Phishing Example

From: “Client Content Filter System" <client-web-filter@FAKEBUTLOOKSREAL.org>
Subject: Potential Acceptable Use Violation

Michael,

Our web traffic monitoring service has reported that your account has visited potentially malicious web sites, including sites that are restricted per ABC’s Acceptable Use Policy.

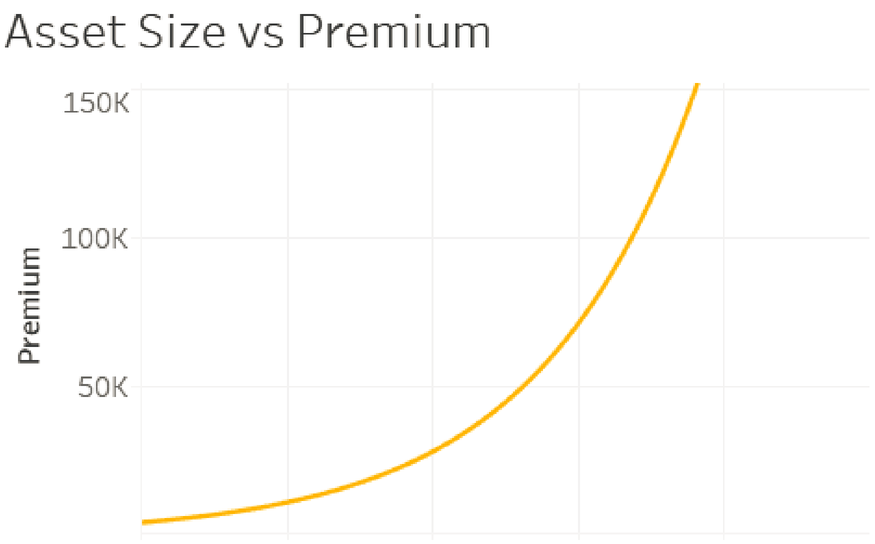
We do realize that this type of activity is often caused by viruses and other types of malware. The following link will direct you to the detailed report of the malicious web sites your system has visited as reported by the monitoring service; please review this list for accuracy.

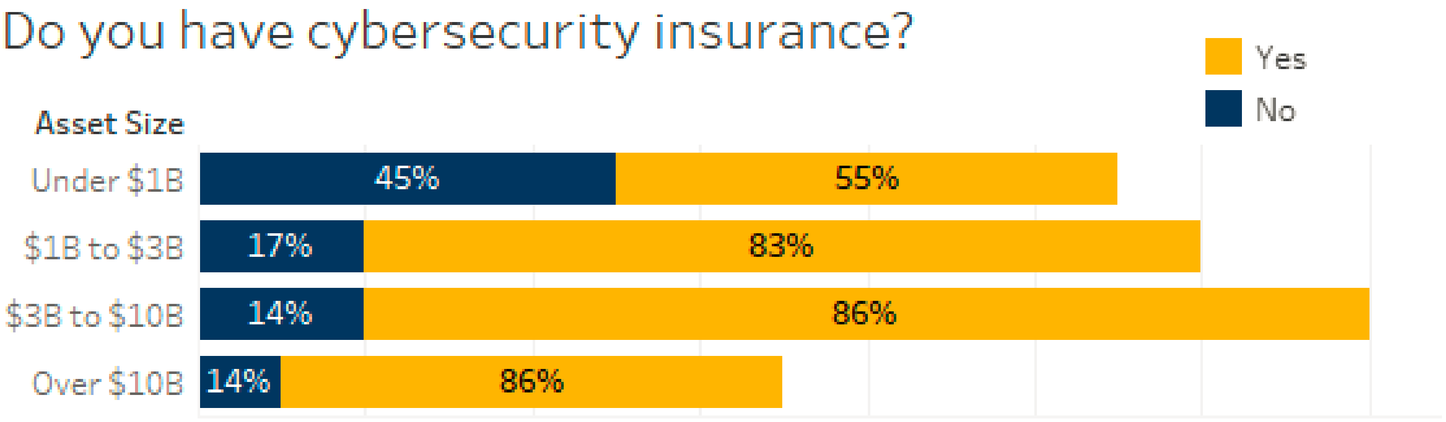
https://www.FAKEBUTLOOKSREAL.org/ABC/?sessionid=ryan.reynolds@abc.com

The file has been encrypted for privacy and requires Microsoft Word macros to be enabled for viewing. If you believe that any of the sites listed in the report have been reported erroneously or that all sites noted are false positives, please reply to this email and a manual review will be conducted by Information Security.

Cybersecurity Insurance

- Crowe performed a Cybersecurity Insurance survey of approximately 50 Banks, questions addressed:
  - Insurance adoption
  - Asset Size vs. Deductible
  - Asset Size vs. Policy Limits
  - Asset Size vs. Premiums
  - Claims Processing


Asset Size vs Premium


Do you have cybersecurity insurance?

What can I do to be more secure?

How do I secure myself: Tips and Tricks

✓Password security – LastPass

✓Use of biometrics – Touch ID

✓If an email doesn’t look right, call somebody

✓What’s in a (domain) name?

✓Anti-virus is good, but isn’t enough

✓Use of Passphrases

✓Don’t let children touch anything!

How do I secure my company: Tips and Tricks

✓Protect your assets through People, Process and Technology controls

✓Establish security and control standards

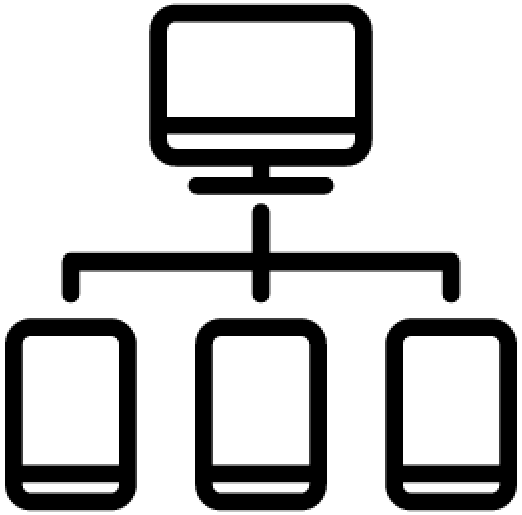
✓Password security

✓Manage your users' permissions

✓Patch systems

✓Monitor your infrastructure

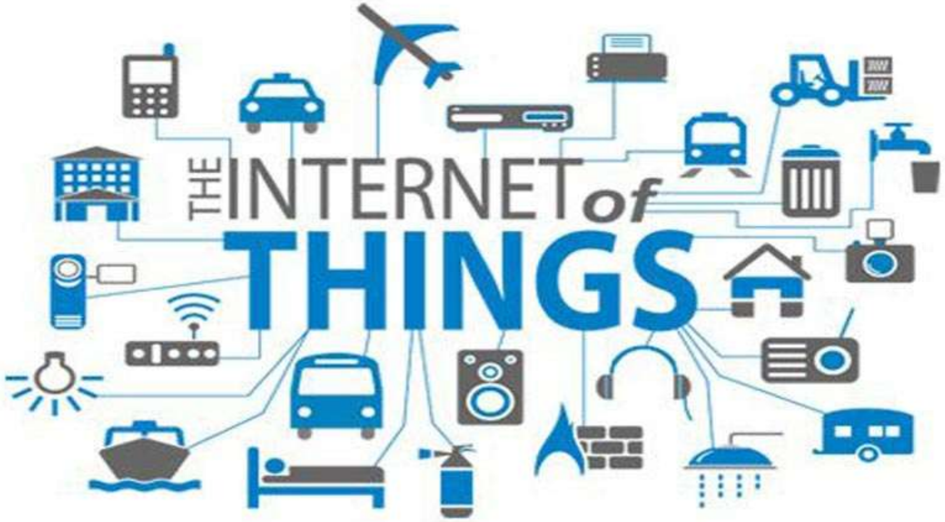
✓**Test your controls!**



Increased Points of Entry

IoT (The Internet of Things)

- 12 billion devices connected to the internet in 2016
- More devices connected than mobile phones by 2018
- By 2020 30 billion devices will be connected
- 5G technology helps enable this expansion
- Benefits
  - Increased productivity
  - Shared us of assets
  - The ability to perform more tasks form almost anywhere
- Concerns
  - Privacy
  - Security



Source: Goldman Sachs, “Ransomware: The 5G Revolution: The Internet of Things Meets Everything,” May 2016
http://www.goldmansachs.com/our-thinking/pages/iot-meets-everything.html?cid=PS_01_35_07_00_01_16_01&mkwid=8luESsWm

Stories from the Field

Questions?

Please connect with me for any questions or additional information:

Michael Lucas
+1(317) 850 3651
Michael.Lucas@crowehorwath.com

In accordance with applicable professional standards, some firm services may not be available to attest clients.

This material is for informational purposes only and should not be construed as financial or legal advice. Please seek guidance specific to your organization from qualified advisers in your jurisdiction.