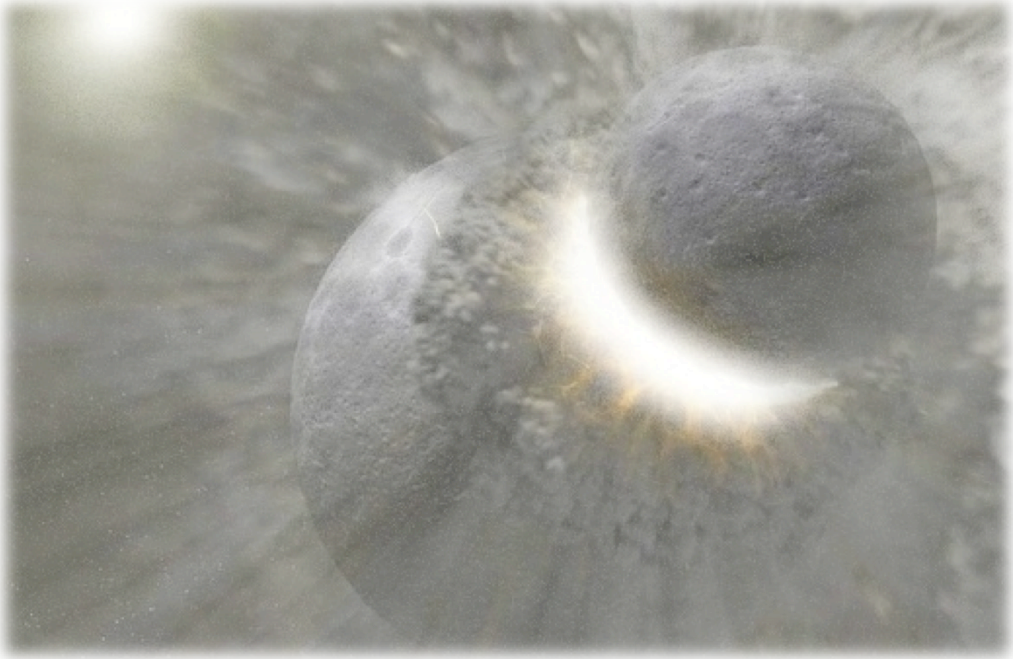
When Business Process & Incident Response Collide

The Fine Tuning of the Incident Response Program



Reneaué Railton
Sr. Information Security Analyst,
Duke Medicine Cyber Defense &
Response

Incident Response

What is the most importance component of an Incident Response Program?

Tools? Processes?

Governance? Policy?

Experience?

Risks to the Organization

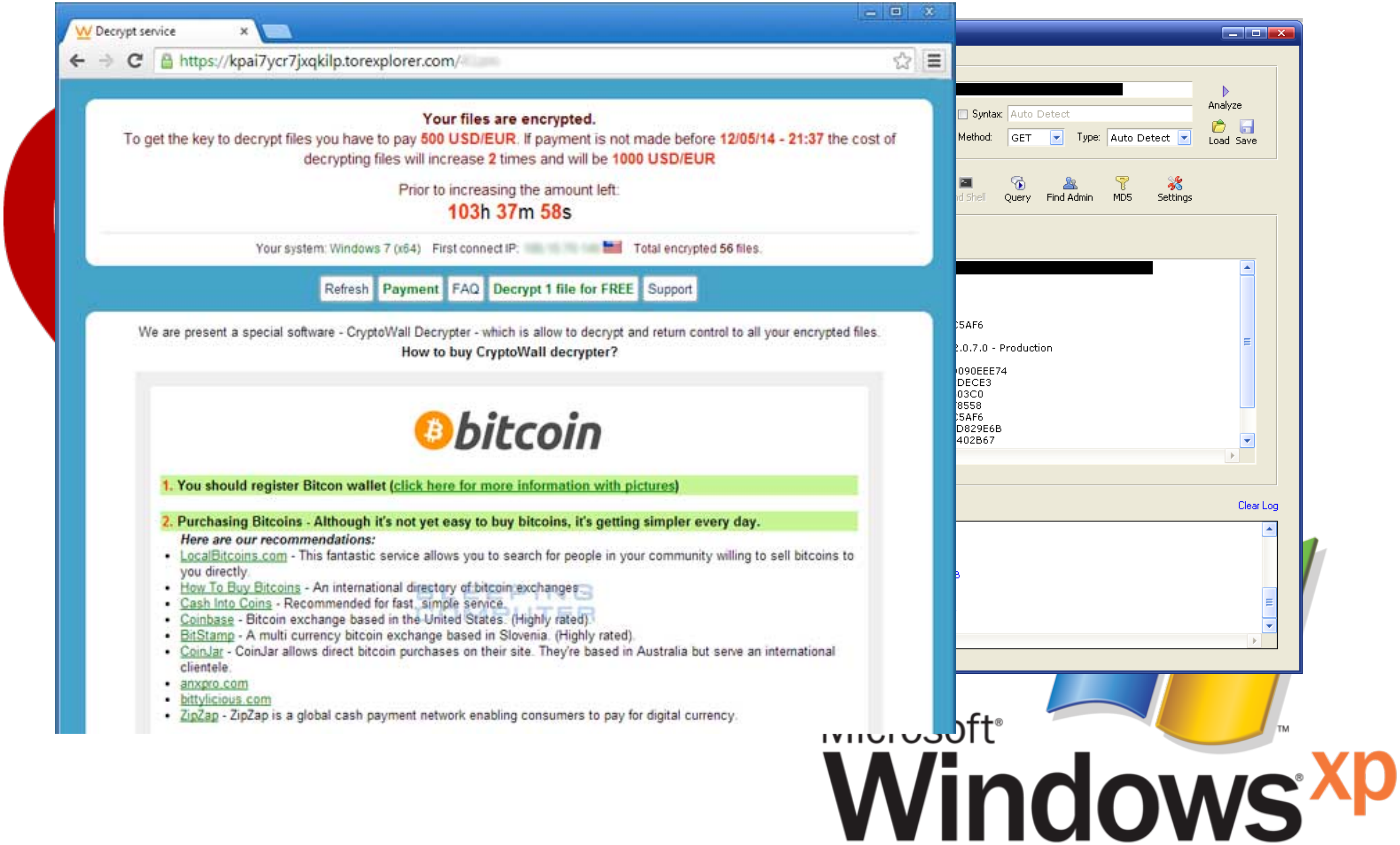
Poor user practices (phishing and insecure data storage)

Inconsistent security practices (adherence to policy ie., exceptions, patching)

Failure to detect attacks (ineffective tools, lack of experience)

Sprawl and amount of data (mobile, remote users, cloud services)

Risks lead to Incidents…



Your files are encrypted.

To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **12/05/14 - 21:37** the cost of decrypting files will increase **2** times and will be **1000 USD/EUR**

Prior to increasing the amount left:

103h 37m 58s

Your system: Windows 7 (x64) First connect IP: [redacted] Total encrypted 56 files.

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

1. **You should register Bitcon wallet (click here for more information with pictures)**
2. **Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.**

Here are our recommendations:

- LocalBitcoins.com - This fantastic service allows you to search for people in your community willing to sell bitcoins to you directly.
- How To Buy Bitcoins - An international directory of bitcoin exchanges.
- Cash Into Coins - Recommended for fast, simple service.
- Coinbase - Bitcoin exchange based in the United States. (Highly rated).
- BitStamp - A multi currency bitcoin exchange based in Slovenia. (Highly rated).
- CoinJar - CoinJar allows direct bitcoin purchases on their site. They're based in Australia but serve an international clientele.
- anxpro.com
- bittylicious.com
- ZipZap - ZipZap is a global cash payment network enabling consumers to pay for digital currency.

[redacted]

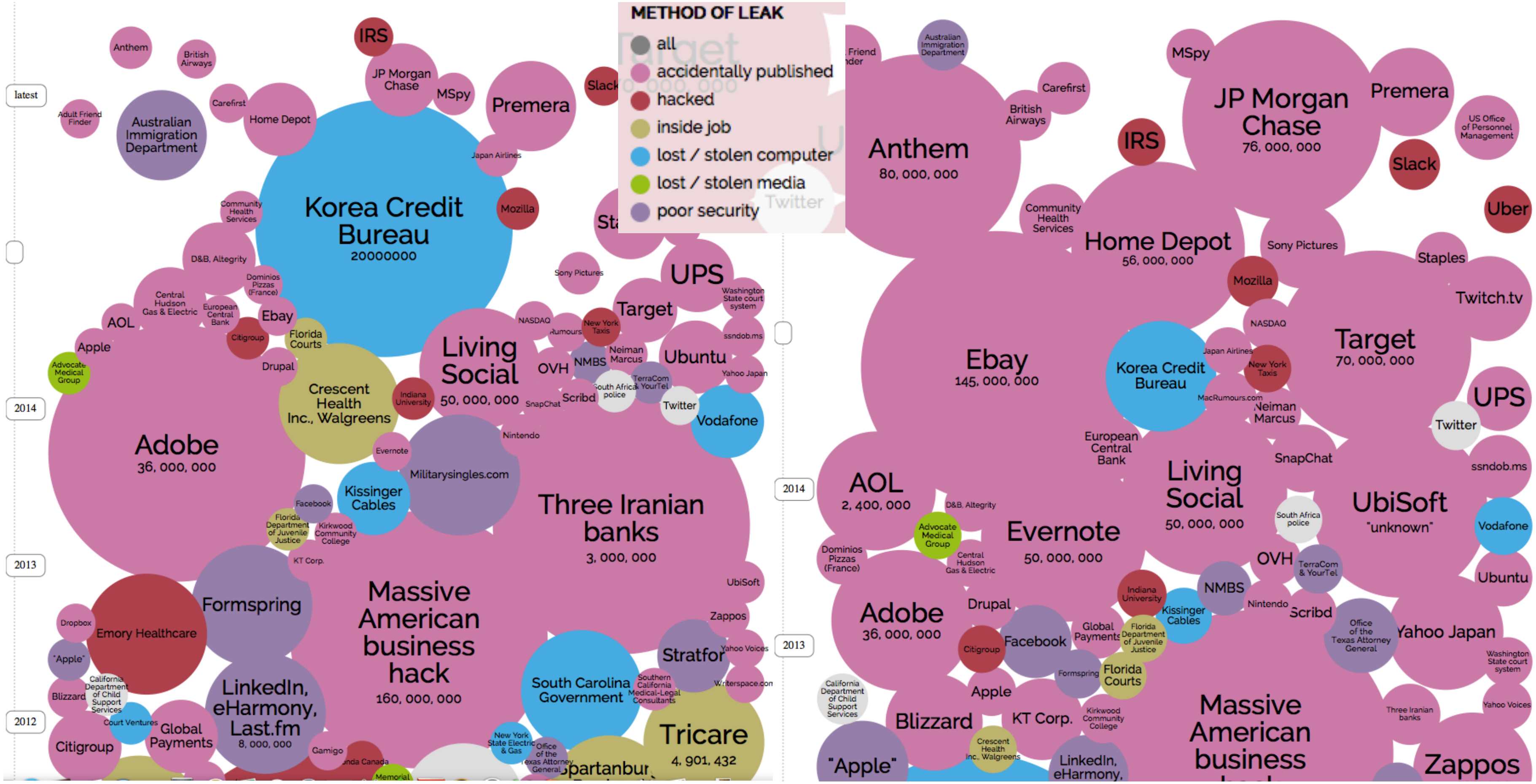
[redacted]

```
C5AF6
2.0.7.0 - Production
090EEE74
DECE3
03C0
8558
C5AF6
D829E6B
402B67
```

Our attack surface is increasing!
We're loosing visibility!
My controls aren't working!!

A Breach is imminent!

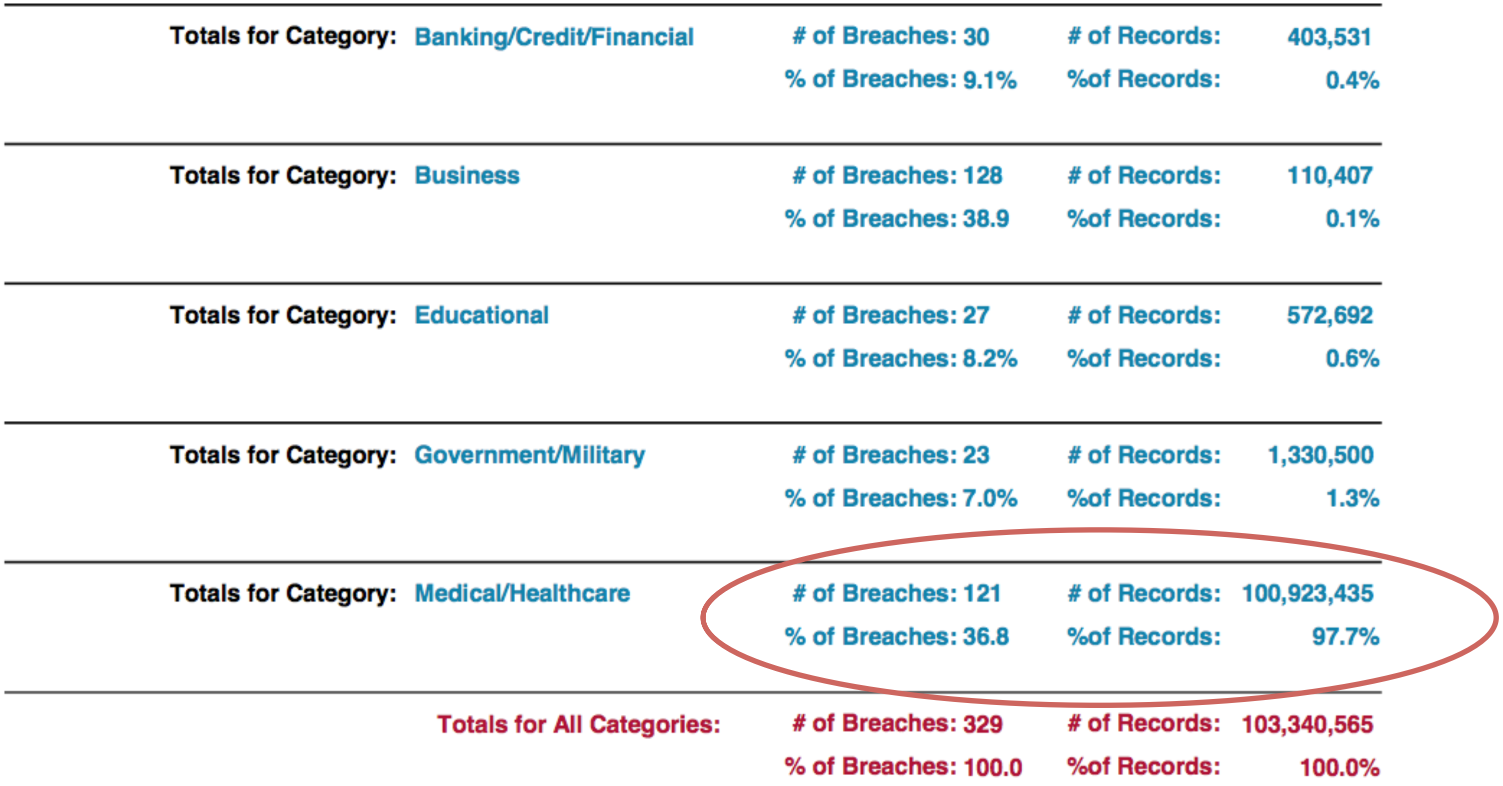
World’s Largest Data Breaches



Breach by data sensitivity

Breach by number of records stolen

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



Totals for Category:	Banking/Credit/Financial	# of Breaches: 30	# of Records:	403,531
		% of Breaches: 9.1%	%of Records:	0.4%
Totals for Category:	Business	# of Breaches: 128	# of Records:	110,407
		% of Breaches: 38.9	%of Records:	0.1%
Totals for Category:	Educational	# of Breaches: 27	# of Records:	572,692
		% of Breaches: 8.2%	%of Records:	0.6%
Totals for Category:	Government/Military	# of Breaches: 23	# of Records:	1,330,500
		% of Breaches: 7.0%	%of Records:	1.3%
Totals for Category:	Medical/Healthcare	# of Breaches: 121	# of Records:	100,923,435
		% of Breaches: 36.8	%of Records:	97.7%
Totals for All Categories:		# of Breaches: 329	# of Records:	103,340,565
		% of Breaches: 100.0	%of Records:	100.0%

Identity Theft Resource Center

2015 Data Breach Category Summary
Report Date: 6/2/2015

http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf

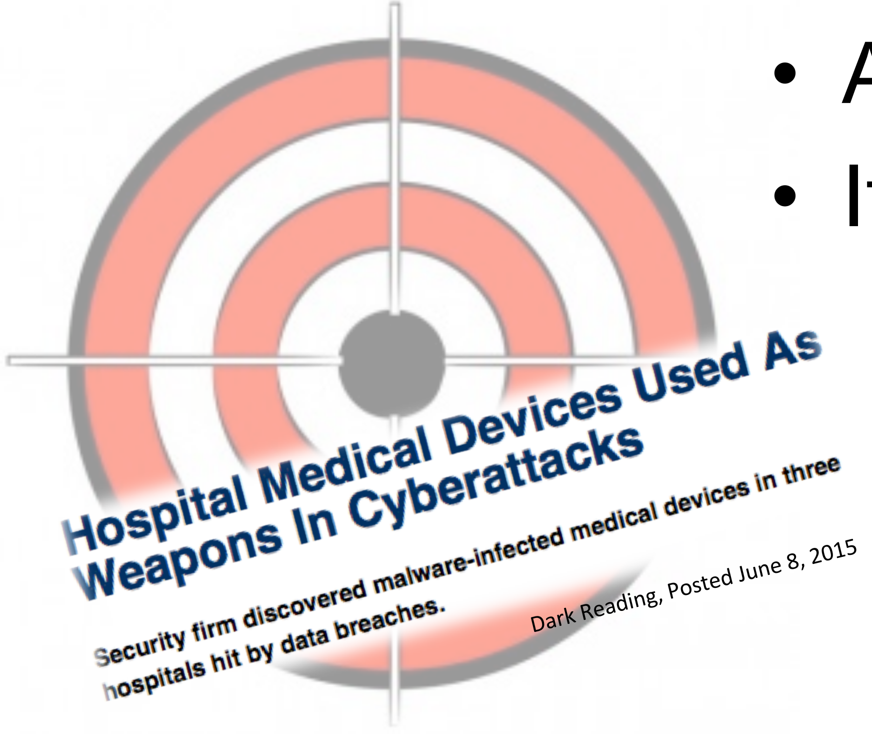
Ponemon 2015 Benchmark Study on Privacy & Security of Healthcare Data

- 90% of Healthcare organizations in the study experienced a breach
- 40% had 5 or more data breaches over 2 years
- Estimated average cost of healthcare breach over $2.1 million
- Criminal attacks are the #1 cause of data breaches in Healthcare
- Attacks are up 125% compared to 5 years ago

Threats

What can we do?

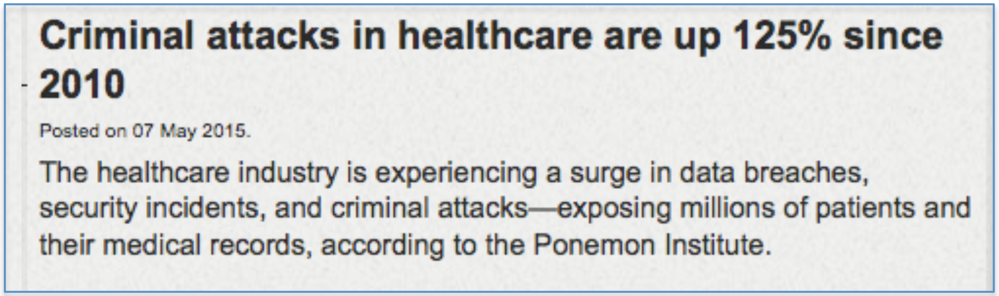
- We're under attack right now!
- Attackers are winning!
- It's getting worse!



Hospital Medical Devices Used As Weapons In Cyberattacks

Security firm discovered malware-infected medical devices in three hospitals hit by data breaches.

Dark Reading, Posted June 8, 2015



Criminal attacks in healthcare are up 125% since 2010

Posted on 07 May 2015.

The healthcare industry is experiencing a surge in data breaches, security incidents, and criminal attacks—exposing millions of patients and their medical records, according to the Ponemon Institute.

What is our current focus?

Compromised Accounts

- Log Analysis with Splunk

Vulnerable Systems

- Vulnerability scanning and remediation

Firewall

Compromised Systems

- Log analysis and network data

SourceFire IPS

Firewall

NetFlow

Sensitive Data

- Data loss prevention technologies and policy

Scaling the Response?

- Incident Response Program needs to be 24/7
- Automation only works on "known quantities"
- How do we make the argument for better tools or more resources?

Who Provides the Response?

Organizational CSIRT

- Costs to own and maintain equipment
- Salary & Benefits
- Training
- Localized, Site specific

Pros

- Understanding of network environment
- Reports are unique to situation

Outside Security Service

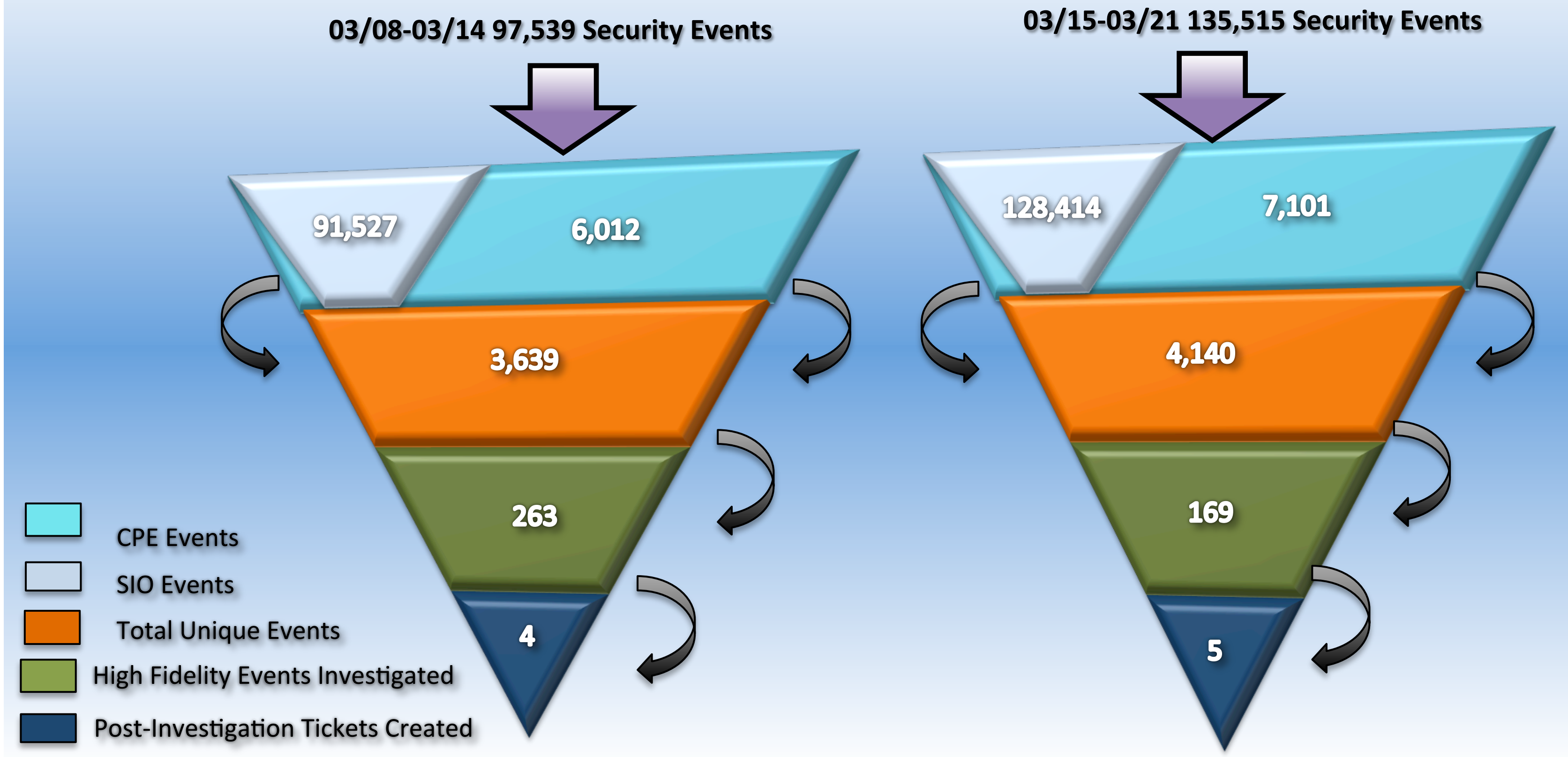
- Equipment provided and maintained by third party
- Data and Intelligence aggregation across multiple customers
- Identifies Priority events

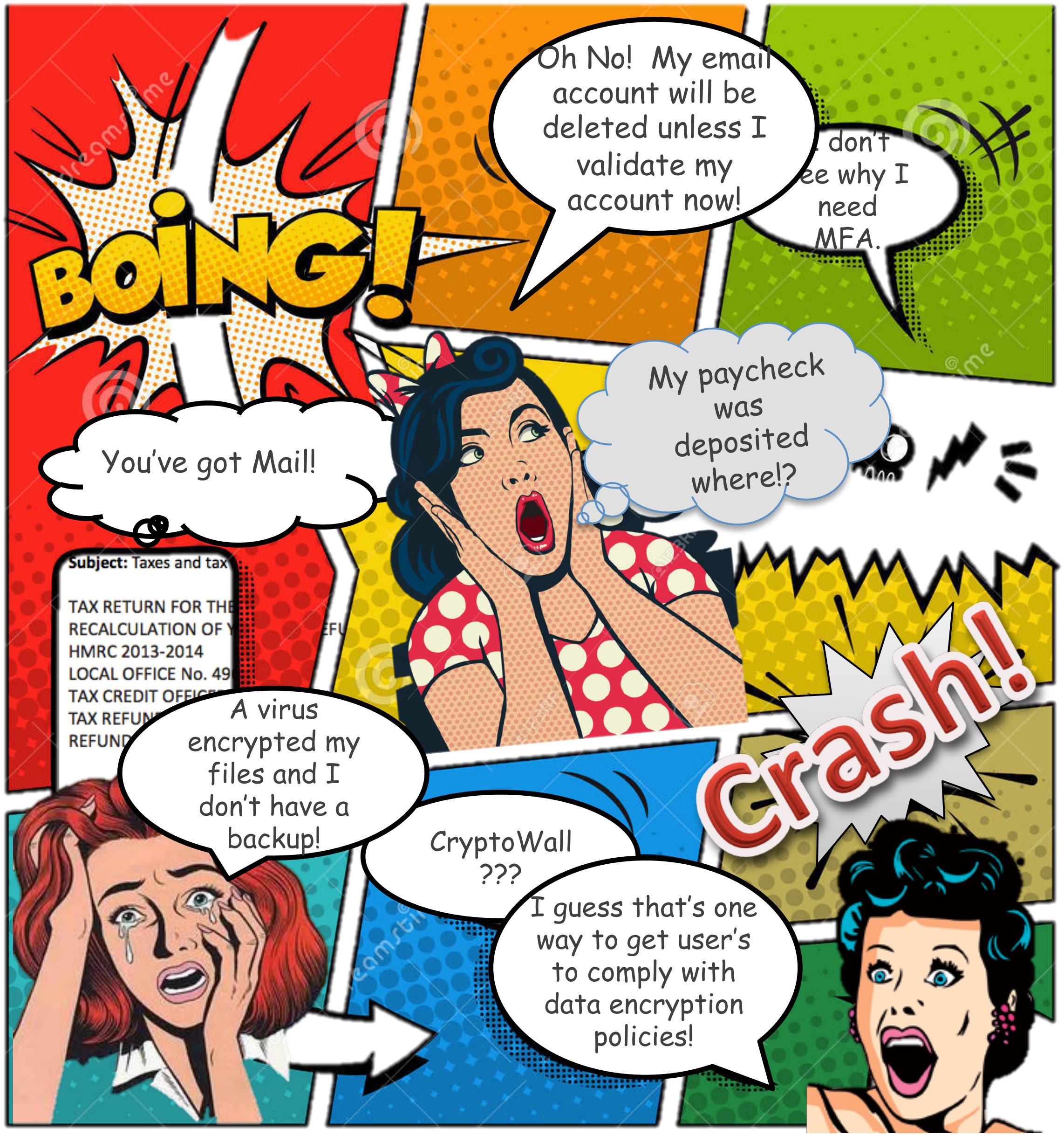
Cons:

- Canned Responses
- Intel provided may not be site specific

Cisco MTD

Duke Medicine statistics 03/08 – 03/31



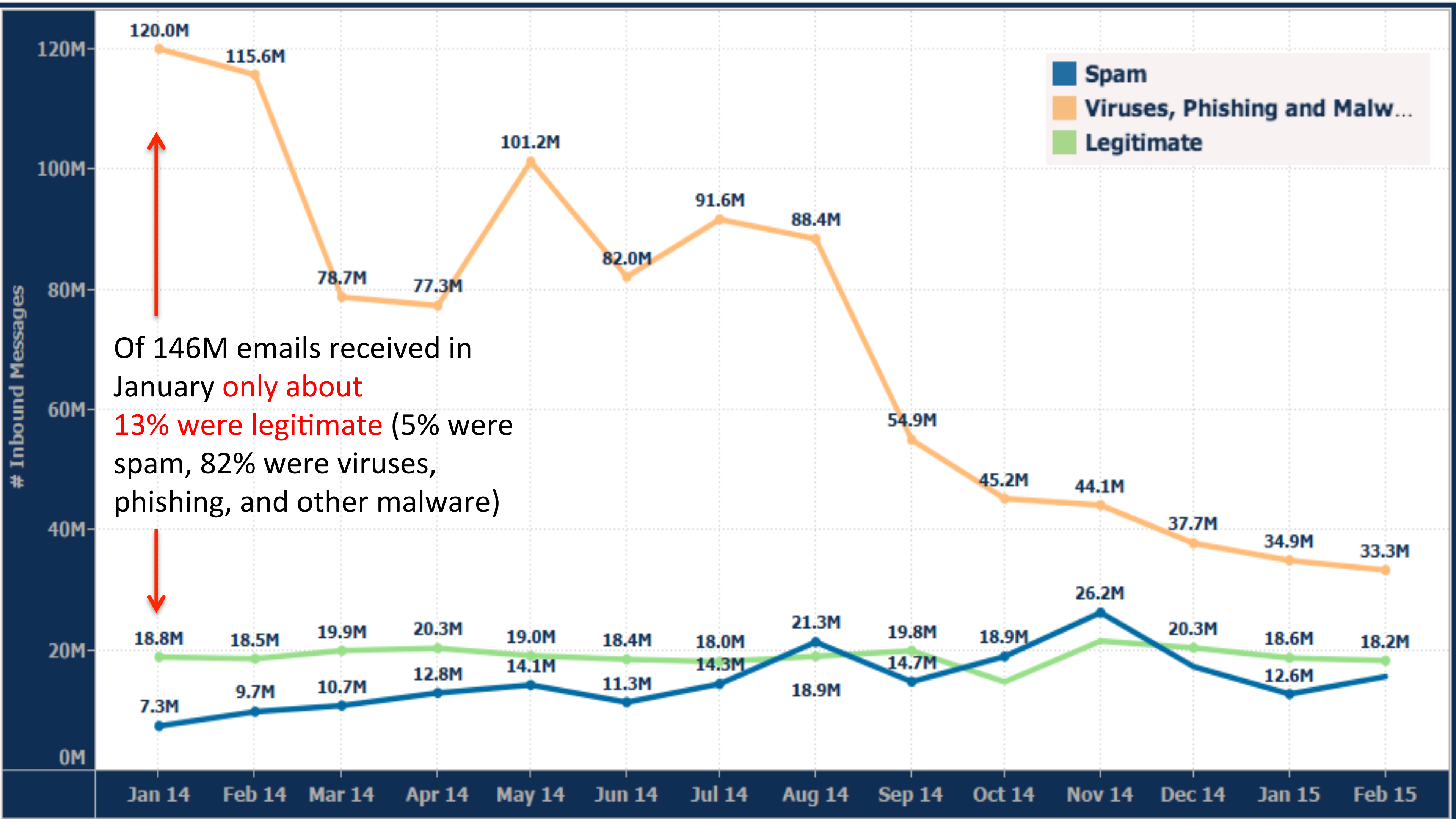

BOING!
Oh No! My email account will be deleted unless I validate my account now!
I don't ee why I need MFA.
You've got Mail!
My paycheck was deposited where!?
Subject: Taxes and tax
TAX RETURN FOR THE
RECALCULATION OF Y
HMRC 2013-2014
LOCAL OFFICE No. 49
TAX CREDIT OFFIC
TAX REFUN
REFUND
EFU
A virus encrypted my files and I don't have a backup!
Crash!
CryptoWall ???
I guess that's one way to get user's to comply with data encryption policies!

Case Study

Email Attacks

Systems processed > 4.7M emails per day at peak;

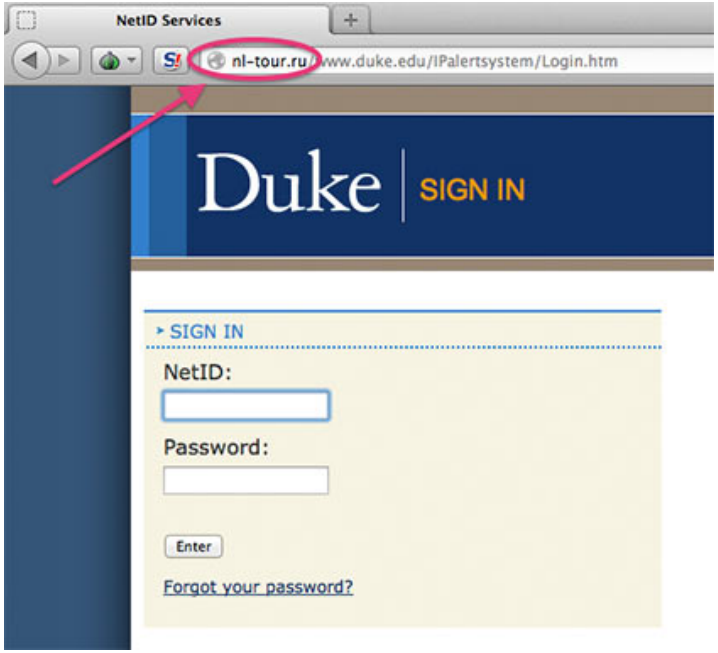
4.5M malicious emails were deleted each day (>3000/minute)



Of 146M emails received in January only about 13% were legitimate (5% were spam, 82% were viruses, phishing, and other malware)

The Phish

- November, 2013: Phishing email sent to 380 users with the subject "Duke Alert" asking them to confirm login details.
- Link lead to Fake Duke Login Page:



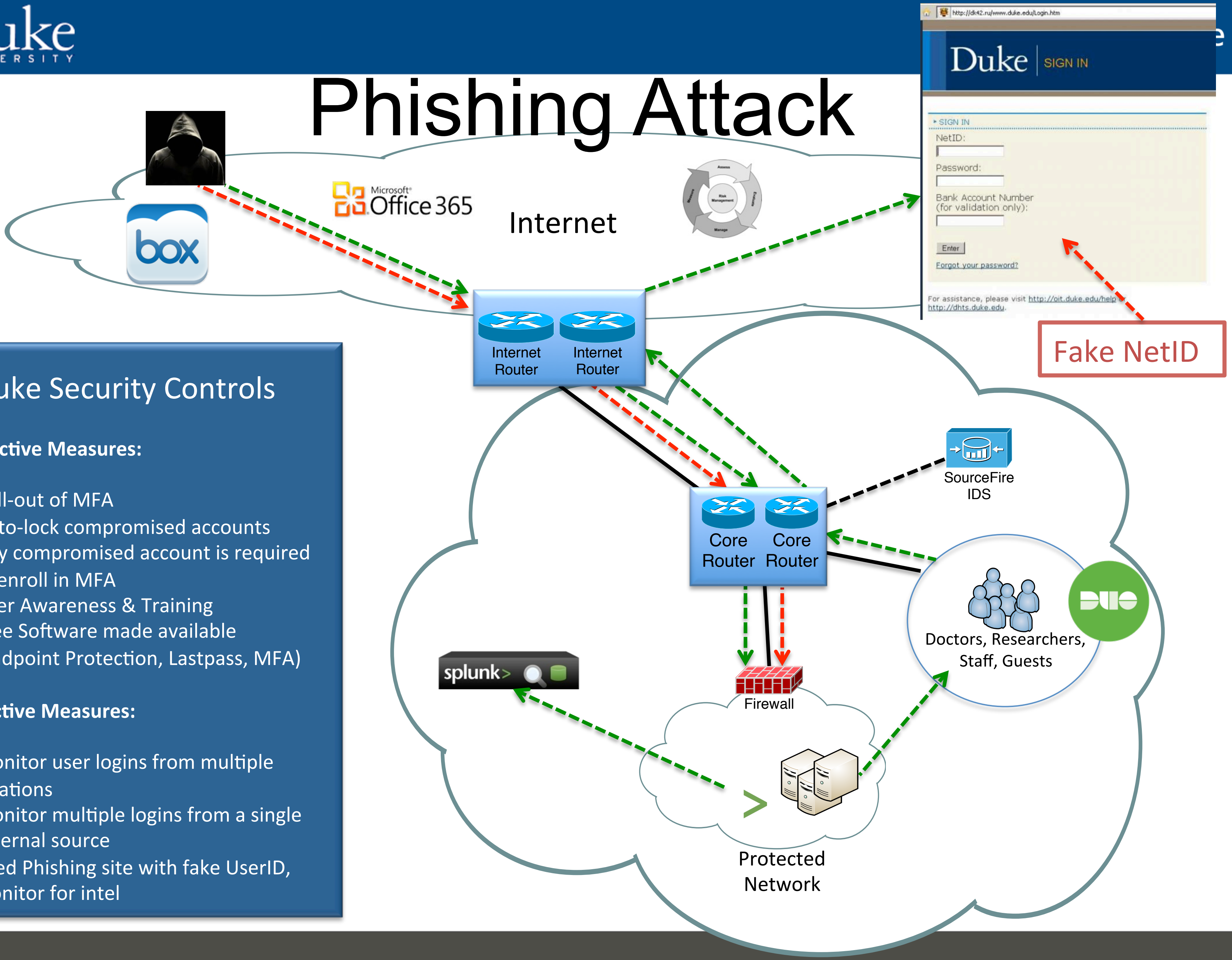
- December, 2013: Employees who had fell for the Phish noticed their paychecks were not deposited on payday – two days before Christmas.
- Investigation found that direct deposits for these employees had been routed to a foreign banking institution in Mauritius.

Who bears the loss?

- The organization who owns the application that was accessed?
- The user who provided their credentials to the criminal.

Employees are paid monthly. If an employee makes 60K/year, that is $5,000 – taxes & insurance. If take home pay is $4000 x 6 employees the loss is minimal at $24000. But what if 100 employees had been affected? 1000?

Phishing Attack



http://dk42.ru/www.duke.edu/Login.htm

Duke | SIGN IN

▸ SIGN IN

NetID:

Password:

Bank Account Number
(for validation only):

Enter

Forgot your password?

For assistance, please visit http://oit.duke.edu/help or http://dhts.duke.edu.

Duke Security Controls

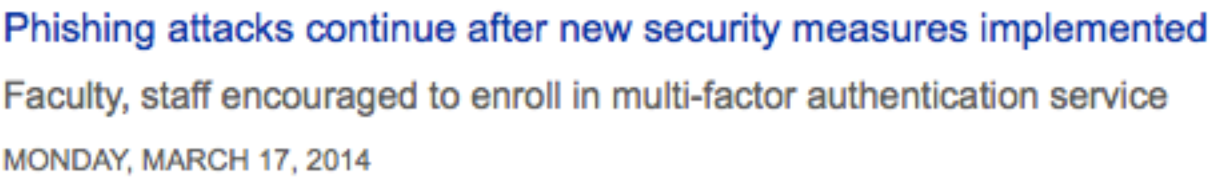
Protective Measures:

- Roll-out of MFA
- Auto-lock compromised accounts
- Any compromised account is required to enroll in MFA
- User Awareness & Training
- Free Software made available (Endpoint Protection, Lastpass, MFA)

Detective Measures:

- Monitor user logins from multiple locations
- Monitor multiple logins from a single external source
- Seed Phishing site with fake UserID, monitor for intel

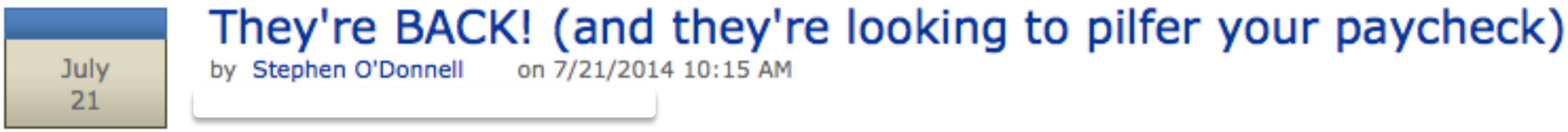
Did it Work?



Phishing attacks continue after new security measures implemented

Faculty, staff encouraged to enroll in multi-factor authentication service

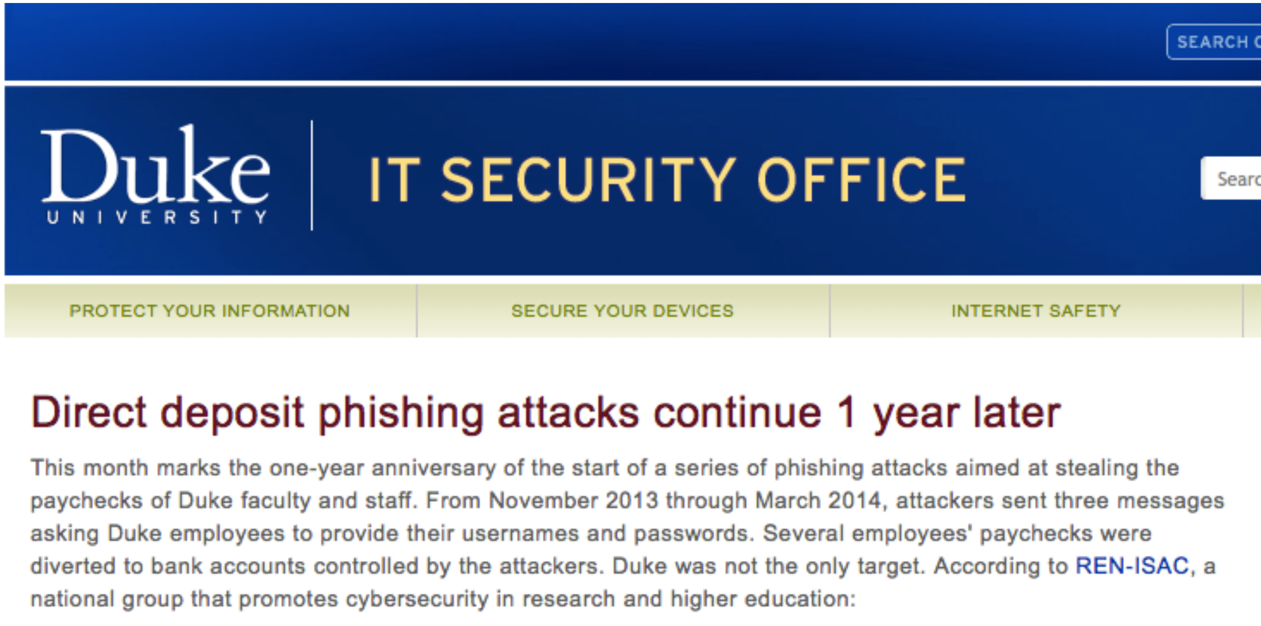
MONDAY, MARCH 17, 2014



They're BACK! (and they're looking to pilfer your paycheck)

by Stephen O'Donnell on 7/21/2014 10:15 AM

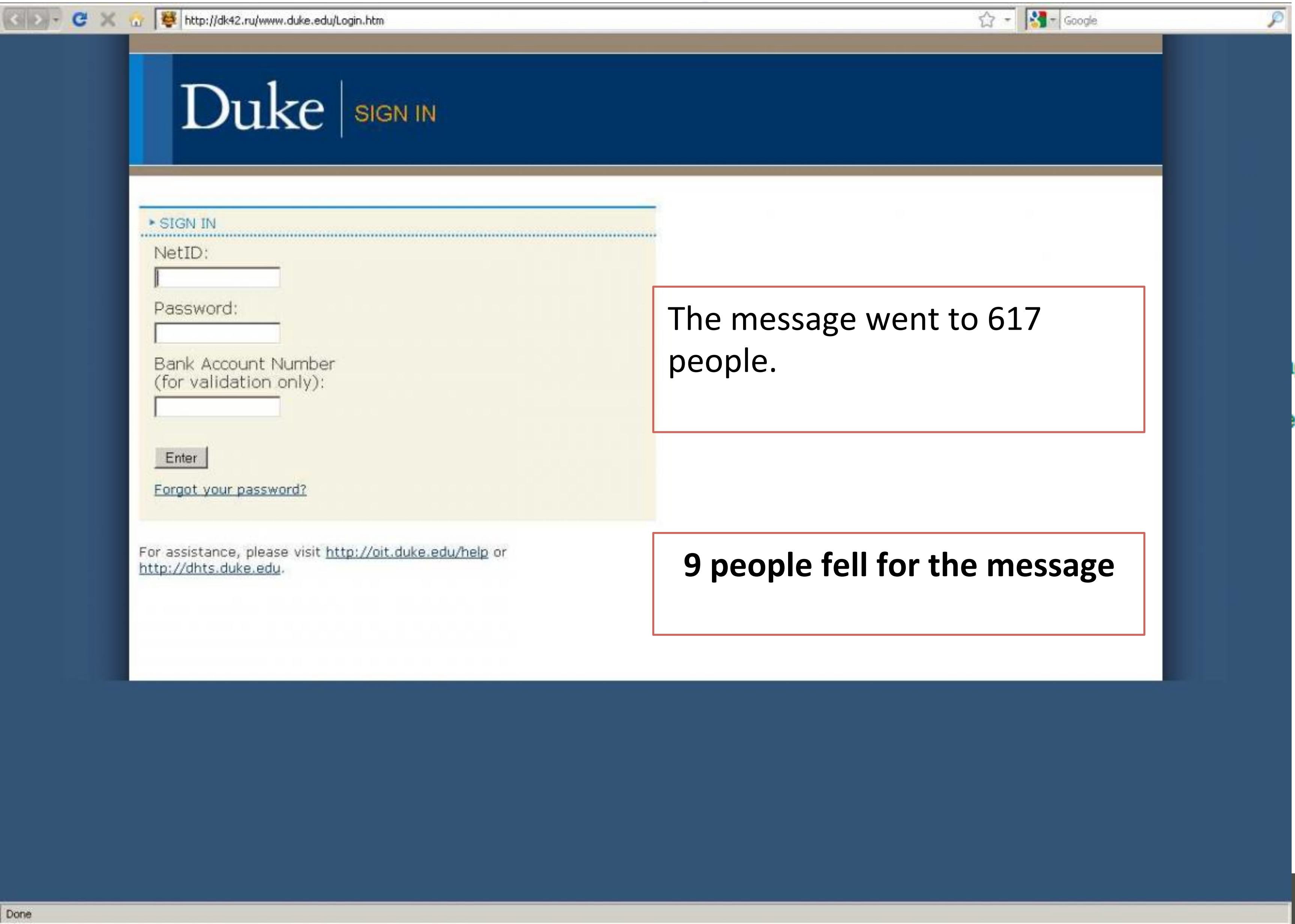
Once again, our IT security
login credentials for the pu
the phishing email promisi
other universities over the



Direct deposit phishing attacks continue 1 year later

This month marks the one-year anniversary of the start of a series of phishing attacks aimed at stealing the paychecks of Duke faculty and staff. From November 2013 through March 2014, attackers sent three messages asking Duke employees to provide their usernames and passwords. Several employees' paychecks were diverted to bank accounts controlled by the attackers. Duke was not the only target. According to REN-ISAC, a national group that promotes cybersecurity in research and higher education:

From: DUKE-HR <employeebenefits@duke.edu>
Date: July 19, 2014 at 10:54:36 AM CDT


http://dk42.ru/www.duke.edu/Login.htm

Duke | SIGN IN

▸ SIGN IN

NetID:

Password:

Bank Account Number
(for validation only):

Enter

Forgot your password?

For assistance, please visit http://oit.duke.edu/help or http://dhts.duke.edu.

Done

The message went to 617 people.

9 people fell for the message

ge of 2.5%

eck.

Weighing the Costs

Before the Incident

- IR Tools
- Trained, experienced staff
- Regular Risk Assessment and Audits

After the Incident

- Third-party Consultants and Investigative Teams
- Technical & Awareness Training
- Recovery/Replacement of damaged assets

Indirect Costs

Intangible Costs

- Damage to Corporate Brand or reputation
- Loss of future customers/ clients/investors

Tangible Costs

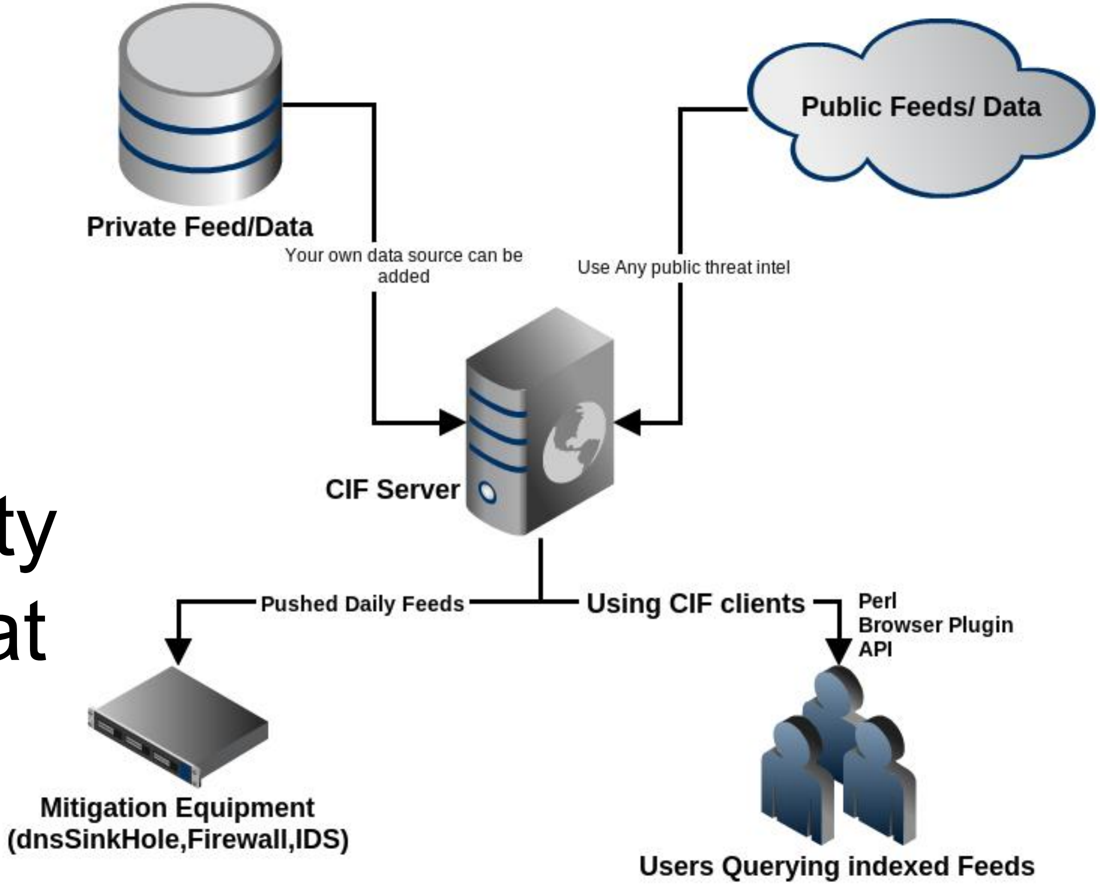
- Regulatory fines
- Loss of Revenue (Sales, productivity, etc.)
- Legal fees
- Identity Protection Services

Security Focus Areas

- Network Security
- System Security
- End User & Account Protection
- Logging & Analysis
- Risk & Governance

Security Defenses and Techniques: Network Security

- NGFW
- VRF Technology
- IPS/IDS utilizing CIF
- Managed Security Services & Threat Defense


Private Feed/Data
Public Feeds/ Data
Your own data source can be added
Use Any public threat intel
CIF Server
Pushed Daily Feeds
Using CIF clients
Perl
Browser Plugin
API
Mitigation Equipment (dnsSinkHole,Firewall,IDS)
Users Querying indexed Feeds

Security Defenses and Techniques: Systems Security

- Automated Patching (IEM)
- Data Loss Prevention (DLP)
- Mobile Device Management
- Web Application Security
- Reduced Administrative Rights

Security Defenses and Techniques: End User and Account Protection

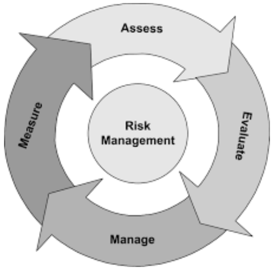
- Whole Disk Encryption
- Spam Filtering
- Endpoint Protection – it’s not just Anti-virus anymore
- Identity and Access Mgt (IAM)
- Secure Sign On Service
- Multifactor authentication (MFA)
- Password Escrow

Security Defenses and Techniques: The Incident Response Toolbag

- Security Information & Event Management (SIEM)
- Threat & Intel Feeds
- NetFlow Analysis
- Log Correlation and Analysis
- Forensics
- Open Source Toolkits

Security Defenses and Techniques: Risk & Governance

- Risk assessments, vulnerability scanning & penetration testing
- Compliance audits
- Policy updates
- Awareness, training and outreach


Assess
Evaluate
Manage
Measure
Risk Management