The NYS Forum, Inc.

Corinne Brennen

Director of Program & Business Development

NYS Forum

SECURITY FRAMEWORKS: EVALUATING MATURITY & CONTINUOUS IMPROVEMENT

George Lazarou, Aspire Technology Partners

USING BIG DATA TO ENSURE COMPLIANCE

Jason Schogel, Splunk

INSIDER THREATS & USER BEHAVIOR ANALYTICS

Jim Kennedy, Varonis

The NYS Forum, Inc.

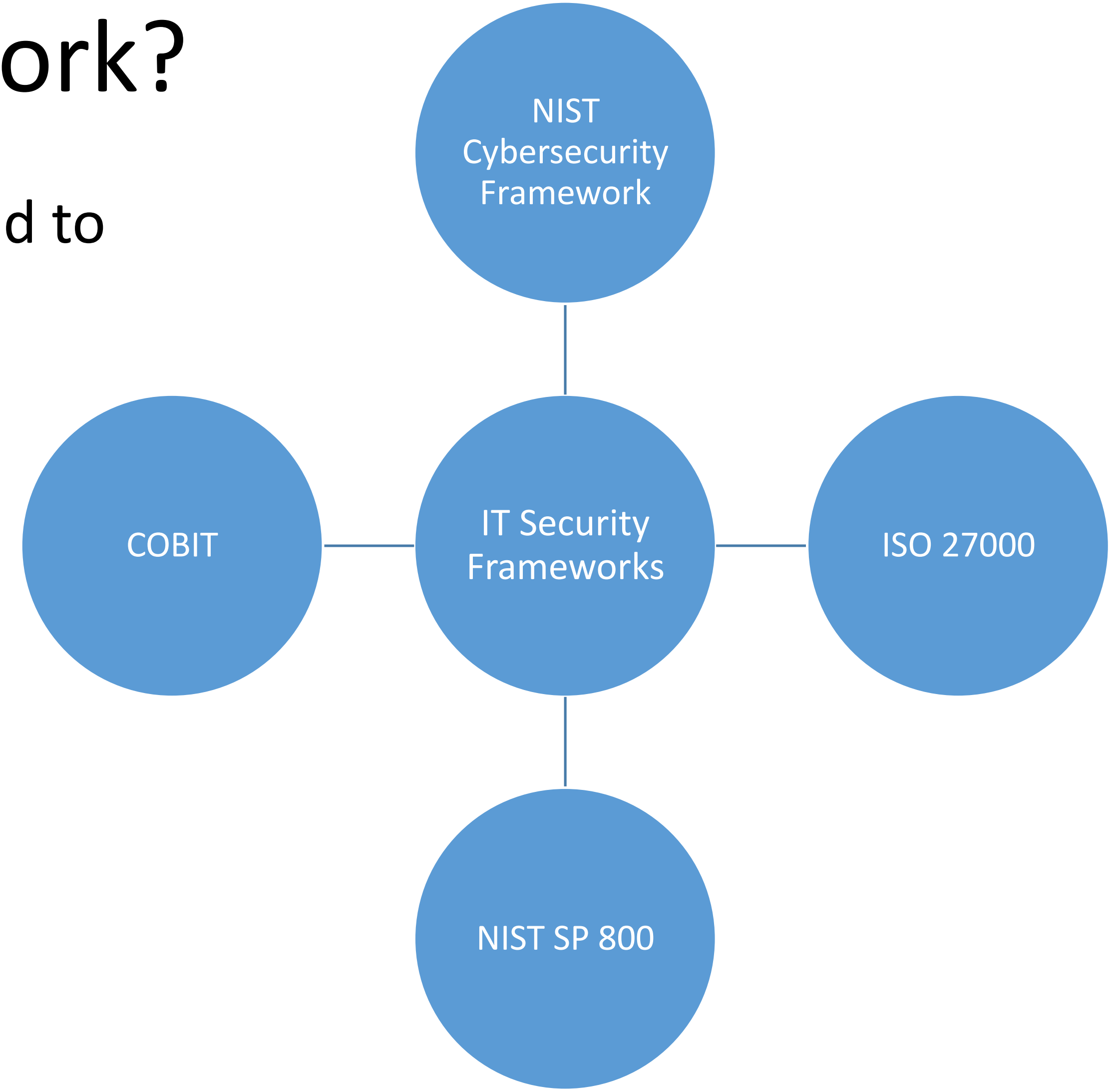
Security Frameworks:

Evaluating Maturity and Continuous Improvement

George Lazarou, CISSP, CGEIT, HCISPP
Principal Security Strategist
Aspire Technology Partners

What is an IT Security Framework?

A series of documented processes that are used to define policies and procedures around the implementation and ongoing management of information security controls in an enterprise environment.



IT Security Frameworks

NIST Cybersecurity Framework

COBIT

ISO 27000

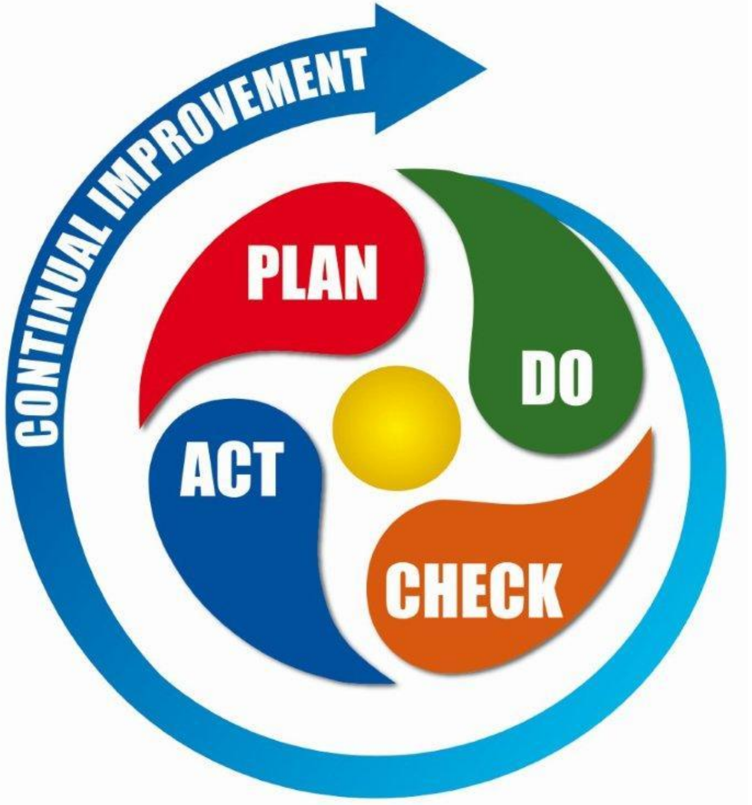
NIST SP 800

What if I don’t work in IT or IT Security?

Organizations rely on Information Technology to process and manage data.

A security framework creates the ability of the organization to communicate the narrative about data protection. Things like who accessed data and applications, where the data resides, and if it leaves the organization are more apparent.

IT Security is a **business** concern, not an IT issue.



How to Prioritize

Identifying How Firms Manage Cybersecurity Investment

- Southern Methodist University, October 2015

Use of Frameworks to Make Budget Case

- Allow CISO to Articulate Where Investments Should be Made
- Used as a Tool to Create a Strategy for Security
- Facilitates the Communication of Strengths and Weakness in Security Program
- **All of the Firms that had a Framework Felt their Budget Was Appropriate**

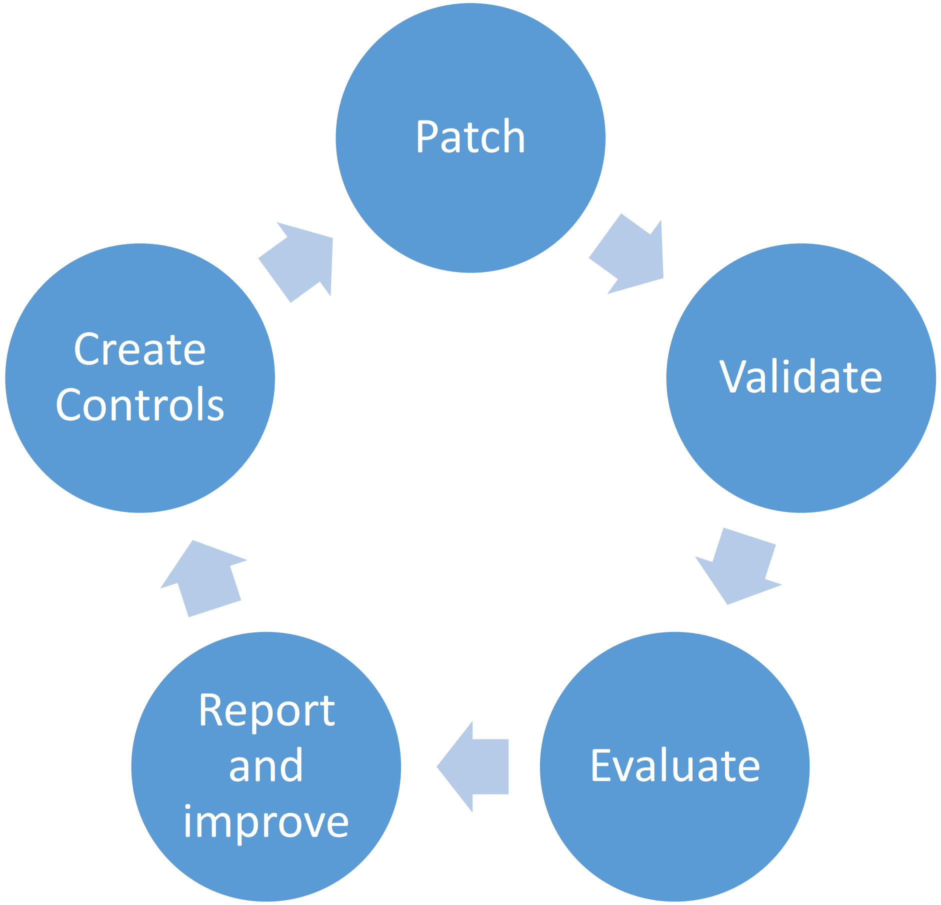
You need to make a process measurable.

PR.IP-12: A vulnerability management plan is developed and implemented	· ISO/IEC 27001:2013 A.12.6.1, A.18.2.2 · NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2

While the controls have a directive, they don't give specifics about measurable criteria.

I.E. All critical security patches will be installed within 45 days.

You can't improve what you can't measure.



The issue is that I don’t know how to get started.

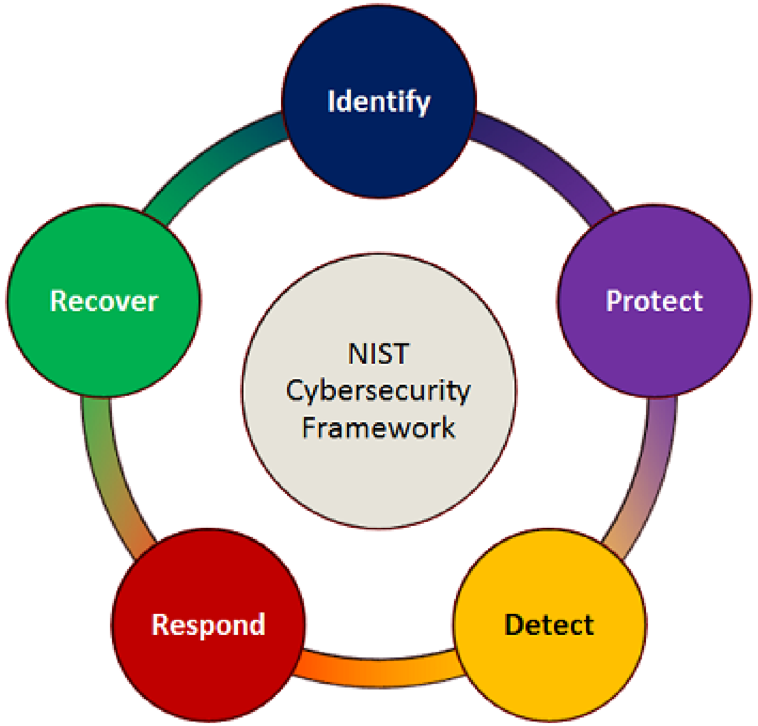
And I don't want this to happen.

NIST Cybersecurity Framework (CSF)

CSF provides an assessment mechanism that enables organizations to determine their current cybersecurity capabilities, set individual goals for a target state, and establish a plan for improving and maintaining cybersecurity programs.

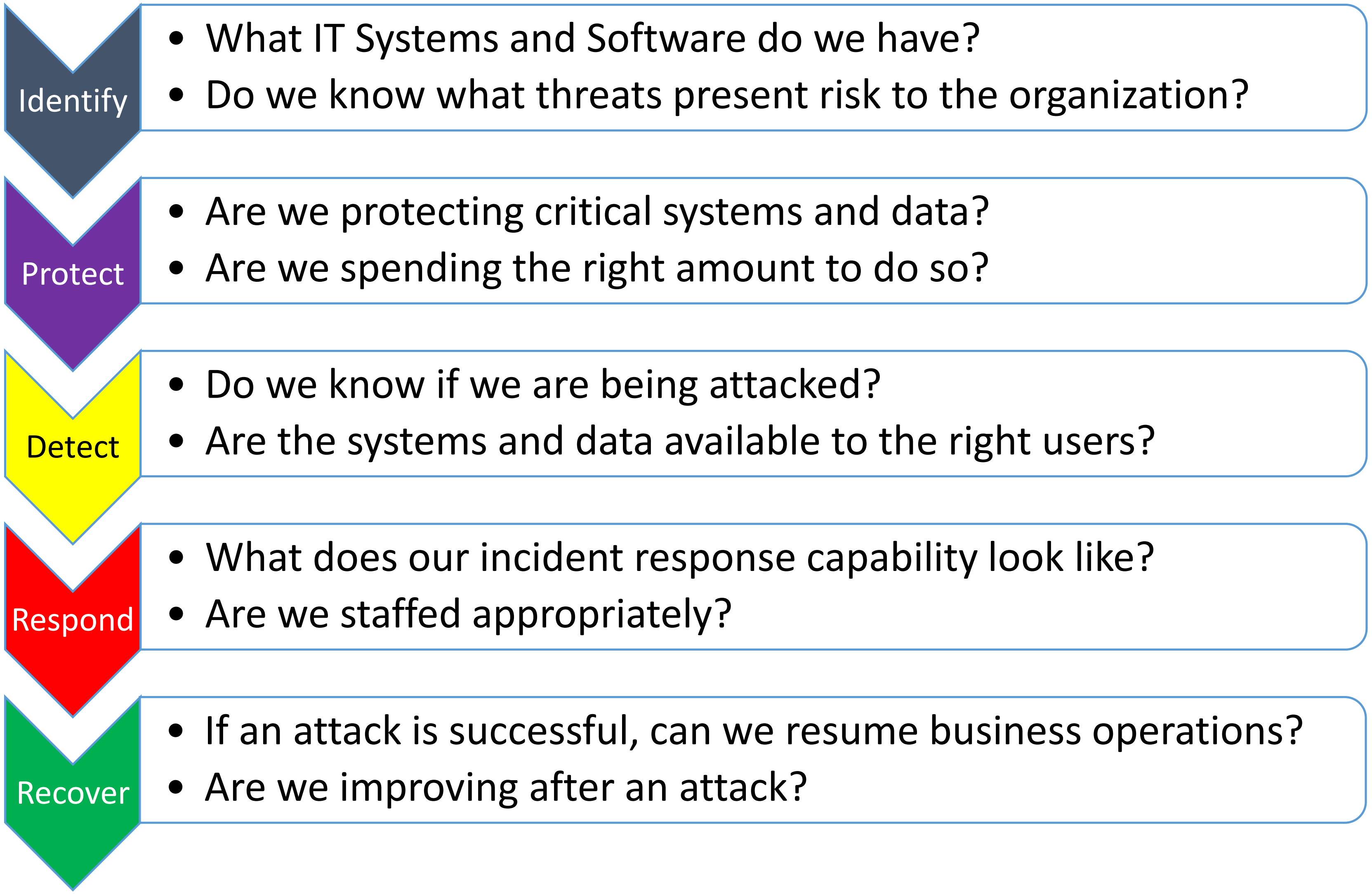
The framework is designed to be a reiterative process that adapts as changes in cybersecurity threats, processes, and technologies evolve.

CSF positions cybersecurity as a dynamic, on-going cycle for continuous improvement.



Are we asking the right questions?

Most organizations spend their time doing what they think needs to be done to protect, generally focusing on products and solutions.



Identify

- What IT Systems and Software do we have?
- Do we know what threats present risk to the organization?

Protect

- Are we protecting critical systems and data?
- Are we spending the right amount to do so?

Detect

- Do we know if we are being attacked?
- Are the systems and data available to the right users?

Respond

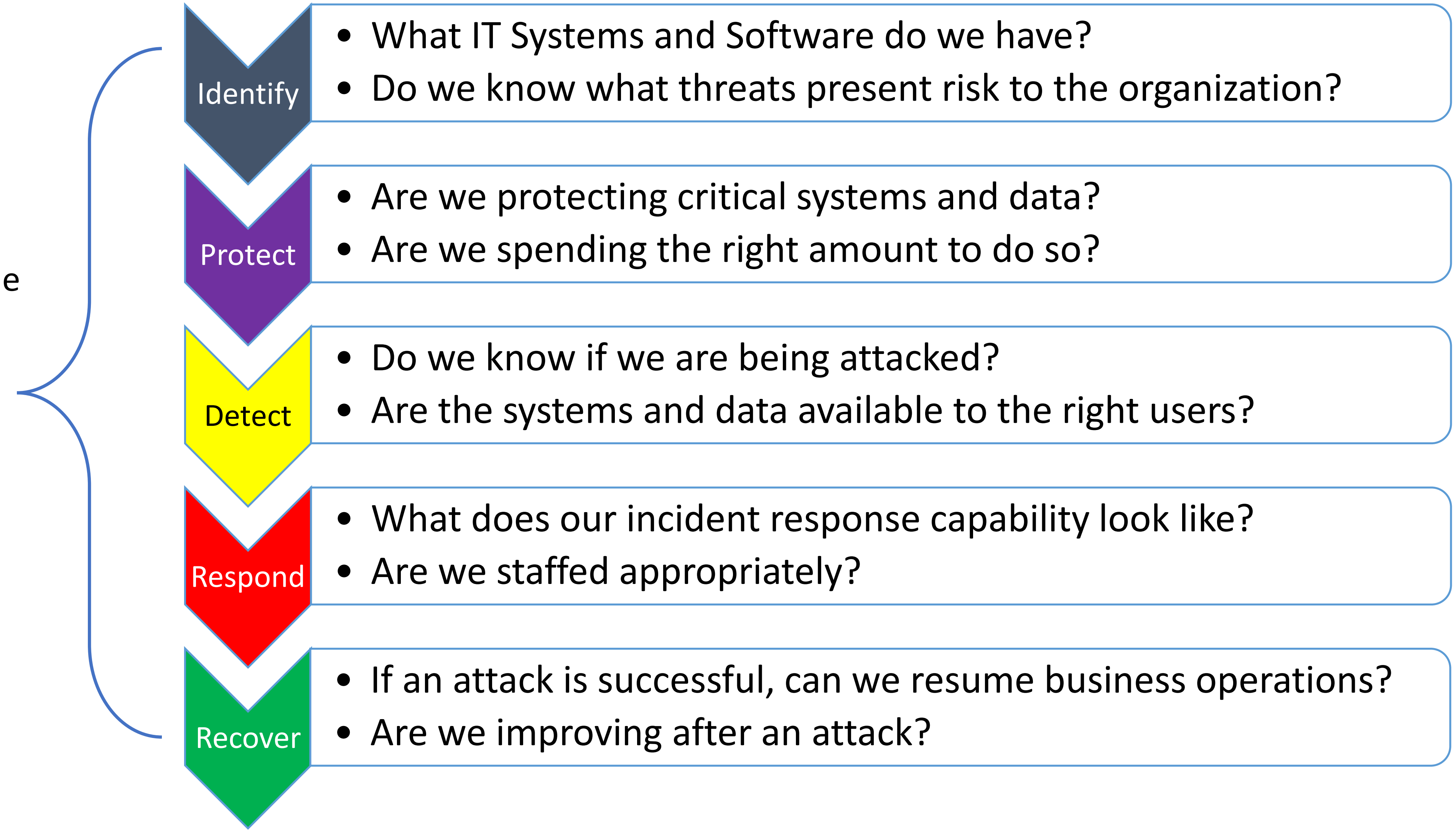
- What does our incident response capability look like?
- Are we staffed appropriately?

Recover

- If an attack is successful, can we resume business operations?
- Are we improving after an attack?

Are we asking the right questions?

And fail to approach the discipline of security with a logical order of operations and in a holistic manner.



Identify

- What IT Systems and Software do we have?
- Do we know what threats present risk to the organization?

Protect

- Are we protecting critical systems and data?
- Are we spending the right amount to do so?

Detect

- Do we know if we are being attacked?
- Are the systems and data available to the right users?

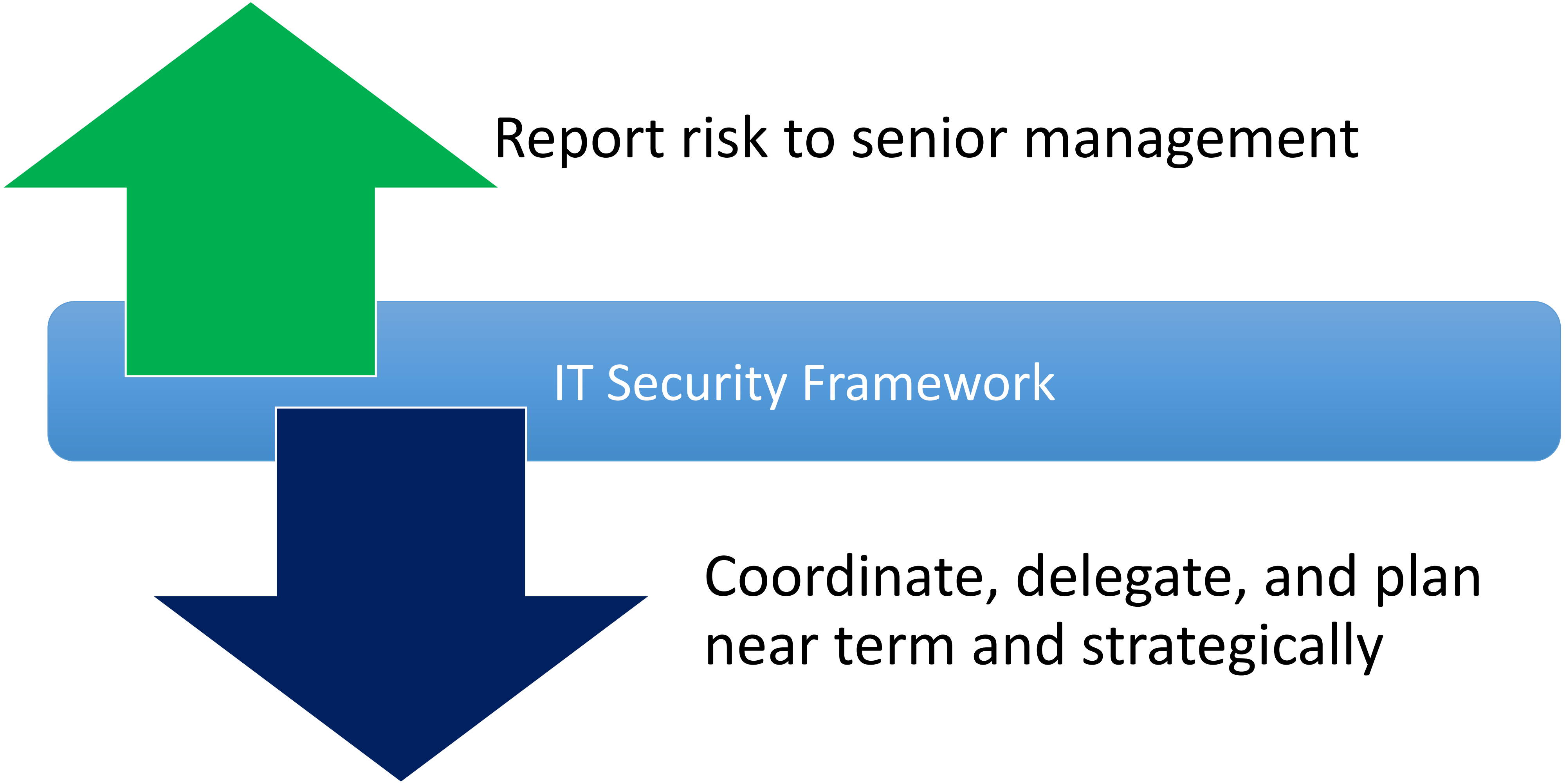
Respond

- What does our incident response capability look like?
- Are we staffed appropriately?

Recover

- If an attack is successful, can we resume business operations?
- Are we improving after an attack?

The bigger picture…



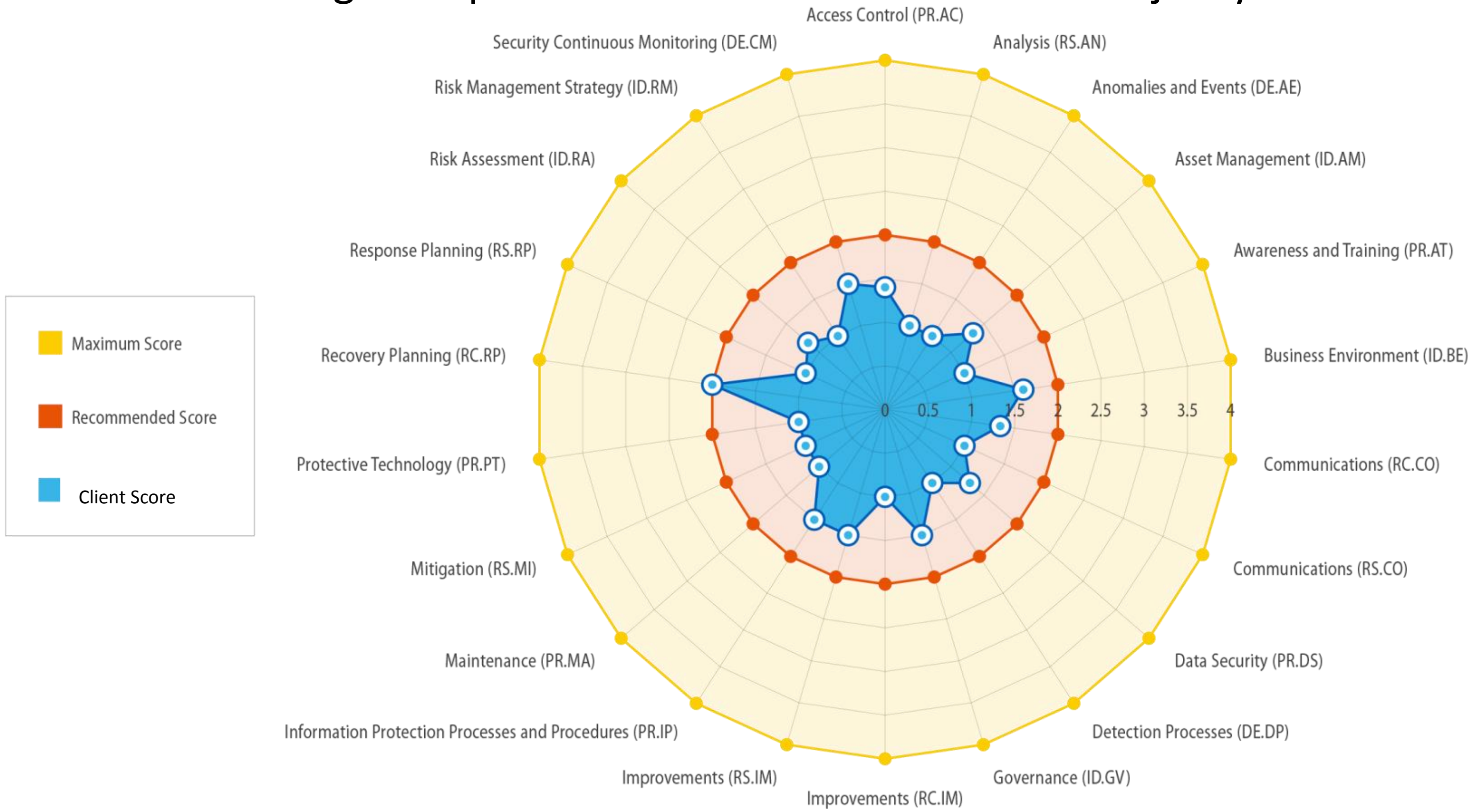
Report risk to senior management

IT Security Framework

Coordinate, delegate, and plan near term and strategically

NIST Cybersecurity Framework (CSF)

The CSF recommends that an organization reach a maturity score of 2 or higher in each area.
The following example falls between 1 and 2 for the majority of the assessed areas.



SECURITY GOVERNANCE	• IT Security Policy Establishment • Risk Management	• Process Enhancement Project • Awareness and Training
DATA SECURITY	• Data Categorization & Information Classification • Data in Transit Encryption Review • Identity & Access Management	• Media Protection • Physical Security Projects • Alternate Work Site Security Controls
SERVER, WORKSTATION & ENDPOINT SECURITY	• Active Directory Project • Data at Rest Encryption	• VOIP Security • Collaboration Security
SECURITY OPERATIONS	• Implement SIEM • Threat & Vulnerability Management	• Secure Maintenance
NETWORK SECURITY	• Network Segmentation • Security Assessments	

Presenter
Aspire Technology Partners
George Lazarou
george@aspiretransforms.com

The NYS Forum, Inc.

Using Big Data for Compliance & Audit

Jason Schogel
Splunk Inc

Compliance Challenges

- Knowing if you're in compliance is difficult
- Assessing the risks and costs can be daunting
- Accessing and correlating information can be tough
- Rules change, as does your environment

Audit Challenges

- Gathering information for the auditor's requests
- Audit failures can be time consuming and costly

Big Data To the Rescue

- Automate the collection and correlation of data for each control
- Let the data answer the questions immediately for the auditor
- Know immediately if you're out of compliance

Compliance Challenges - Understand the Ask

- Different compliance standards call for different controls
- Knowing your controls will help in collecting the right data
  - Pub1075
  - HIPPA
  - CJIS
  - NIST
  - ISO
  - FISMA
  - DFAR
  - Etc

Audit Challenges – Showing an Auditor Your Data

- Gathering records to show an auditor can be daunting task
- Sifting through the data and making acceptable reports is painful
- ***Late fines can be costly***

Examples of Logs Needed:

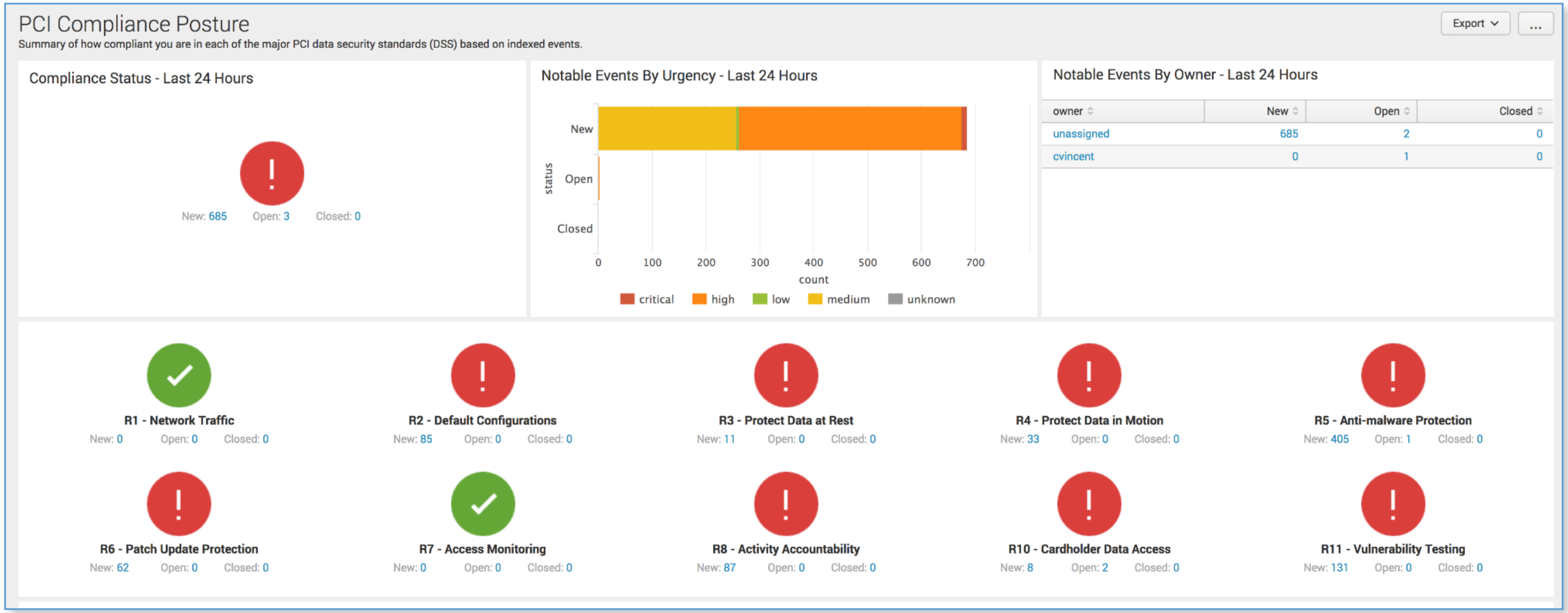
- Firewall logs
- Proxy server logs
- User login records
- File access logs
- Account privilege changes
  Malware/Antivirus scans
- DNS
- Active Directory
- Etc…

Big Data To the Rescue - Automate Data Collection

- The technical aspect of compliance often specifies an entity to ensure the safety of data and data systems
- Much of the technical control data can be automatically collected
  - Failed logins
  - File access
  - Account expiration
  - Server patch levels
  - Antivirus
  - Etc

Big Data To the Rescue - Know if you’re out Of Compliance

- Automate the collection and correlation of data for each control
- Let the data answer the questions immediately for the auditor
- Know ahead of time if you’re not compliant and need other data



PCI Compliance Posture

Summary of how compliant you are in each of the major PCI data security standards (DSS) based on indexed events.

Compliance Status - Last 24 Hours

New: 685 Open: 3 Closed: 0

Notable Events By Urgency - Last 24 Hours

Notable Events By Owner - Last 24 Hours

owner	New	Open	Closed
unassigned	685	2	0
cvincent	0	1	0

R1 - Network Traffic
New: 0 Open: 0 Closed: 0

R2 - Default Configurations
New: 85 Open: 0 Closed: 0

R3 - Protect Data at Rest
New: 11 Open: 0 Closed: 0

R4 - Protect Data in Motion
New: 33 Open: 0 Closed: 0

R5 - Anti-malware Protection
New: 405 Open: 1 Closed: 0

R6 - Patch Update Protection
New: 62 Open: 0 Closed: 0

R7 - Access Monitoring
New: 0 Open: 0 Closed: 0

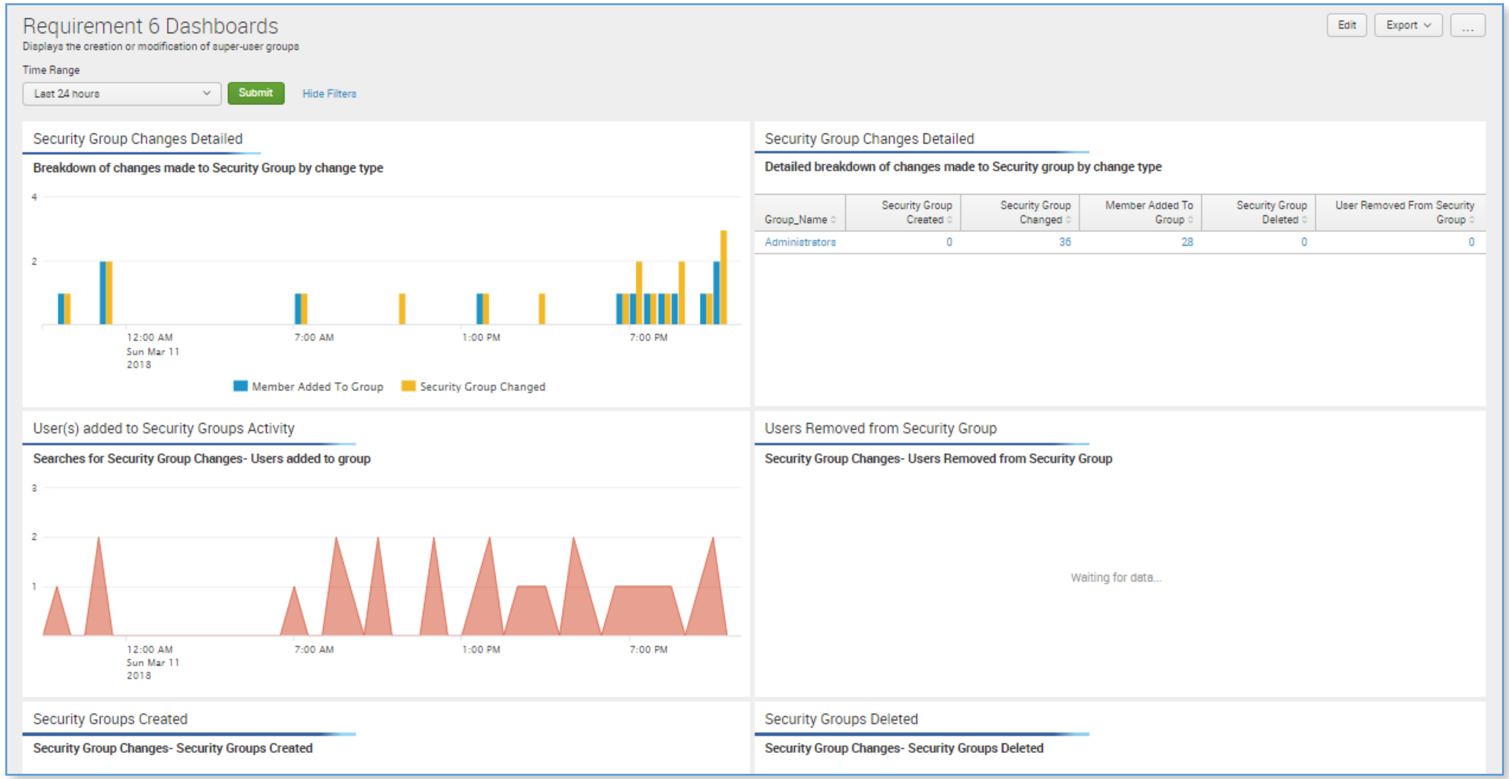
R8 - Activity Accountability
New: 87 Open: 0 Closed: 0

R10 - Cardholder Data Access
New: 8 Open: 2 Closed: 0

R11 - Vulnerability Testing
New: 131 Open: 0 Closed: 0

Big Data To the Rescue - Let the Data Answer the Questions

- Dashboard/Report the information for an auditor’s requests
- Analytics on collected data can show an auditor, control by control



Requirement 6 Dashboards

Displays the creation or modification of super-user groups

Time Range: Last 24 hours

Security Group Changes Detailed

Breakdown of changes made to Security Group by change type

Security Group Changes Detailed

Detailed breakdown of changes made to Security group by change type

Group_Name	Security Group Created	Security Group Changed	Member Added To Group	Security Group Deleted	User Removed From Security Group
Administrators	0	36	28	0	0

User(s) added to Security Groups Activity

Searches for Security Group Changes- Users added to group

Users Removed from Security Group

Security Group Changes- Users Removed from Security Group

Security Groups Created

Security Group Changes- Security Groups Created

Security Groups Deleted

Security Group Changes- Security Groups Deleted

In Summary

- **Audits happen**, so know what you’re supposed to report on
- Collect the data automatically, keeping a historical record
- Display the collected data control by control to make it easy for an auditor, and to know you’re in compliance with the requirements
- Set up alerts for missing data, or periodically check your dashboards to ensure you’ve been collecting without issues
- Work with your IT departments to gain access to the data in an automated fashion, and pull it into a central repository for reporting

Jason Schogel
Sr Sales Engineer
Splunk Inc
jschogel@splunk.com

The NYS Forum, Inc.

Insider Threats & User Behavior Analytics

Jim Kennedy
Varonis

- Threat Landscape
- Insider threats & threat actors
- A few thoughts on ransomware
- User Behavior Analytics
- Mitigating insider threats
- Wrap up/Summary

World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 11th August 2015)

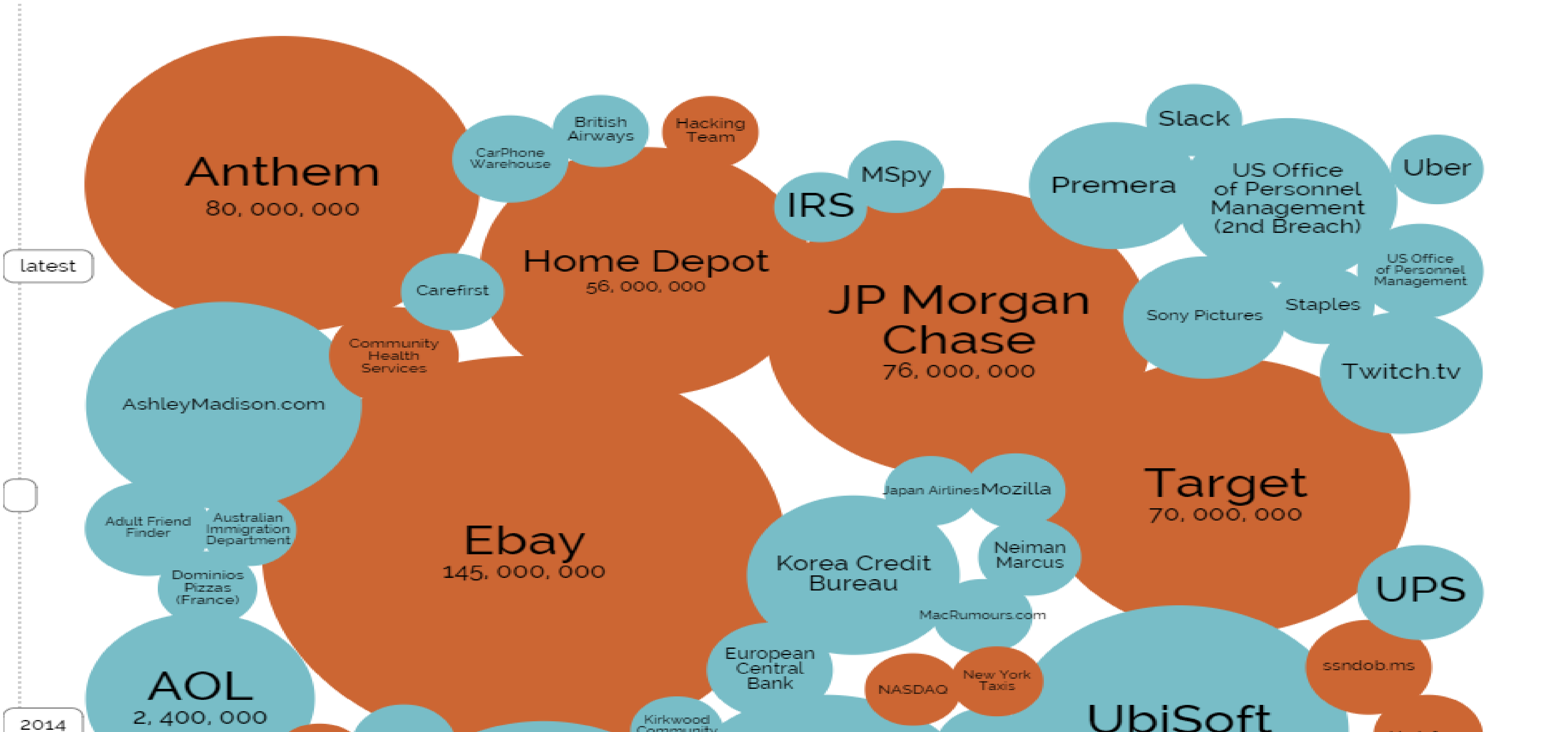
● interesting story

YEAR

BUBBLE COLOUR YEAR | METHOD OF LEAK

BUBBLE SIZE NO OF RECORDS STOLEN | DATA SENSITIVITY

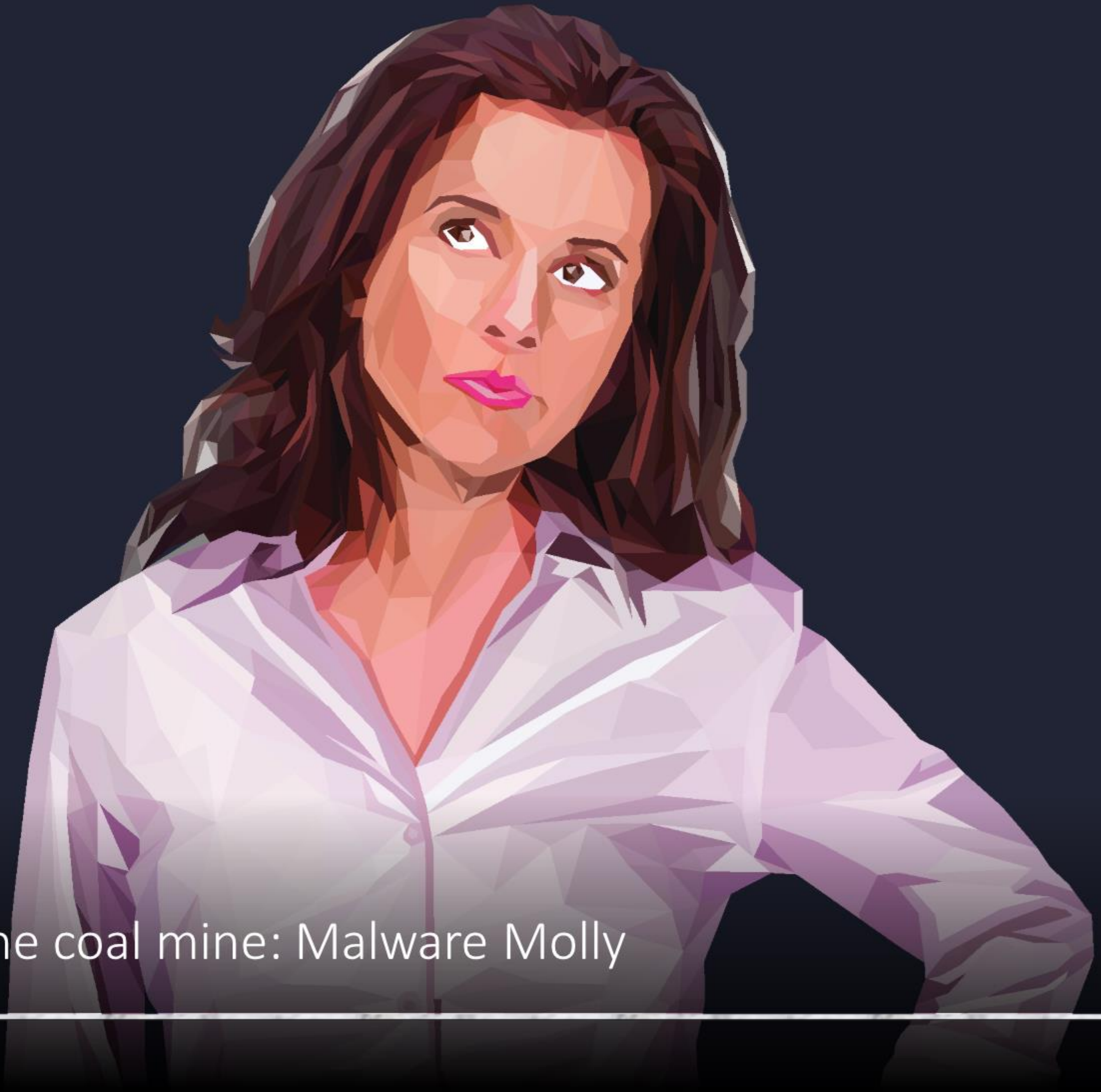
☑ SHOW FILTER



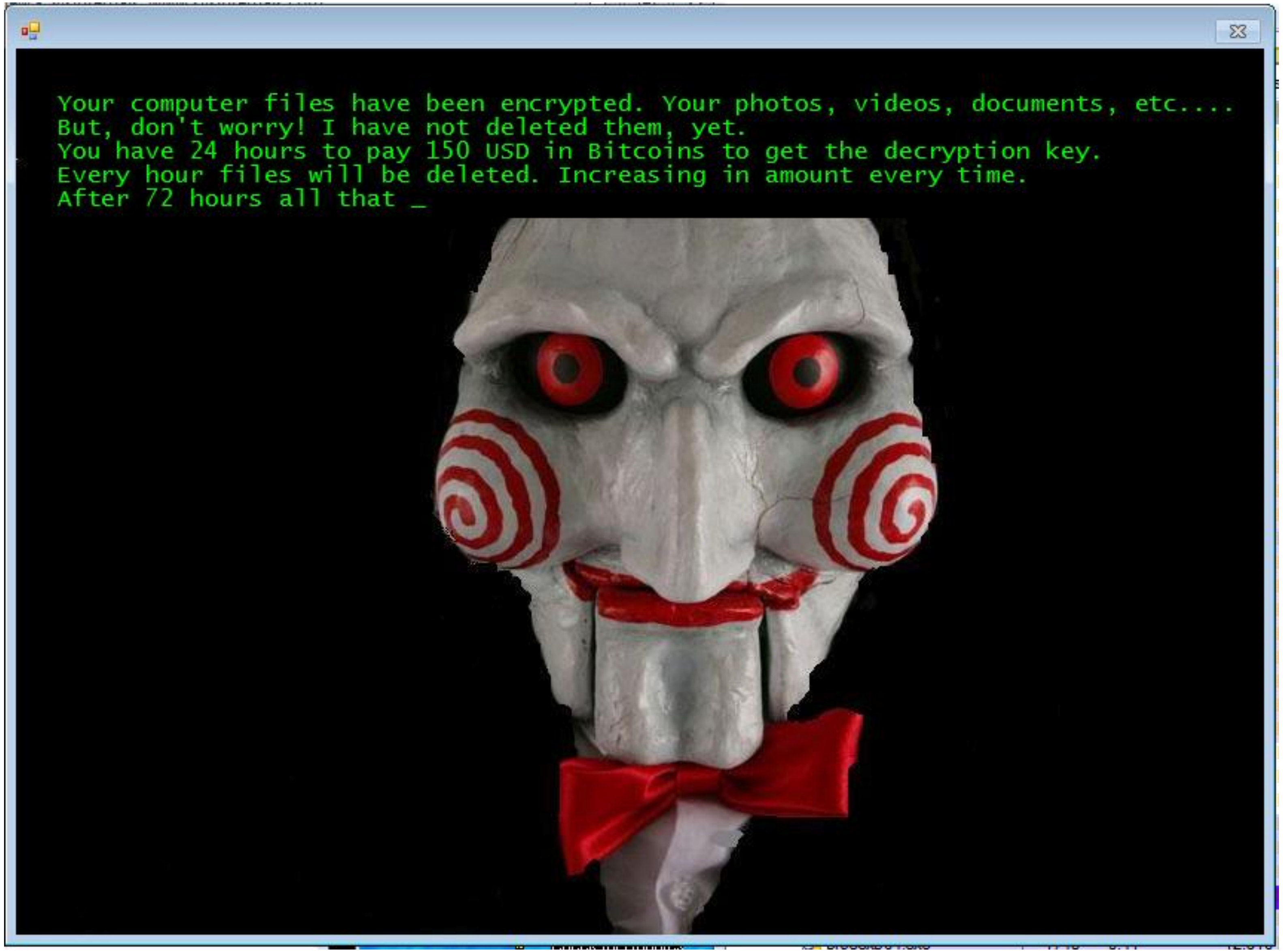
What do many breaches have in common?

- **The threat was already inside**
  - An insider or an attacker that hijacked an insider’s credentials
  - Examples: Snowden, WikiLeaks
- **Unstructured data was leaked, stolen, or used**
  - Documents, spreadsheets, emails, images, videos
  - Examples: Sony, OPM
- **Traditional security approaches didn’t work**
  - Without user behavior analytics, attacks go undetected
  - Examples: Target, Anthem, Sony

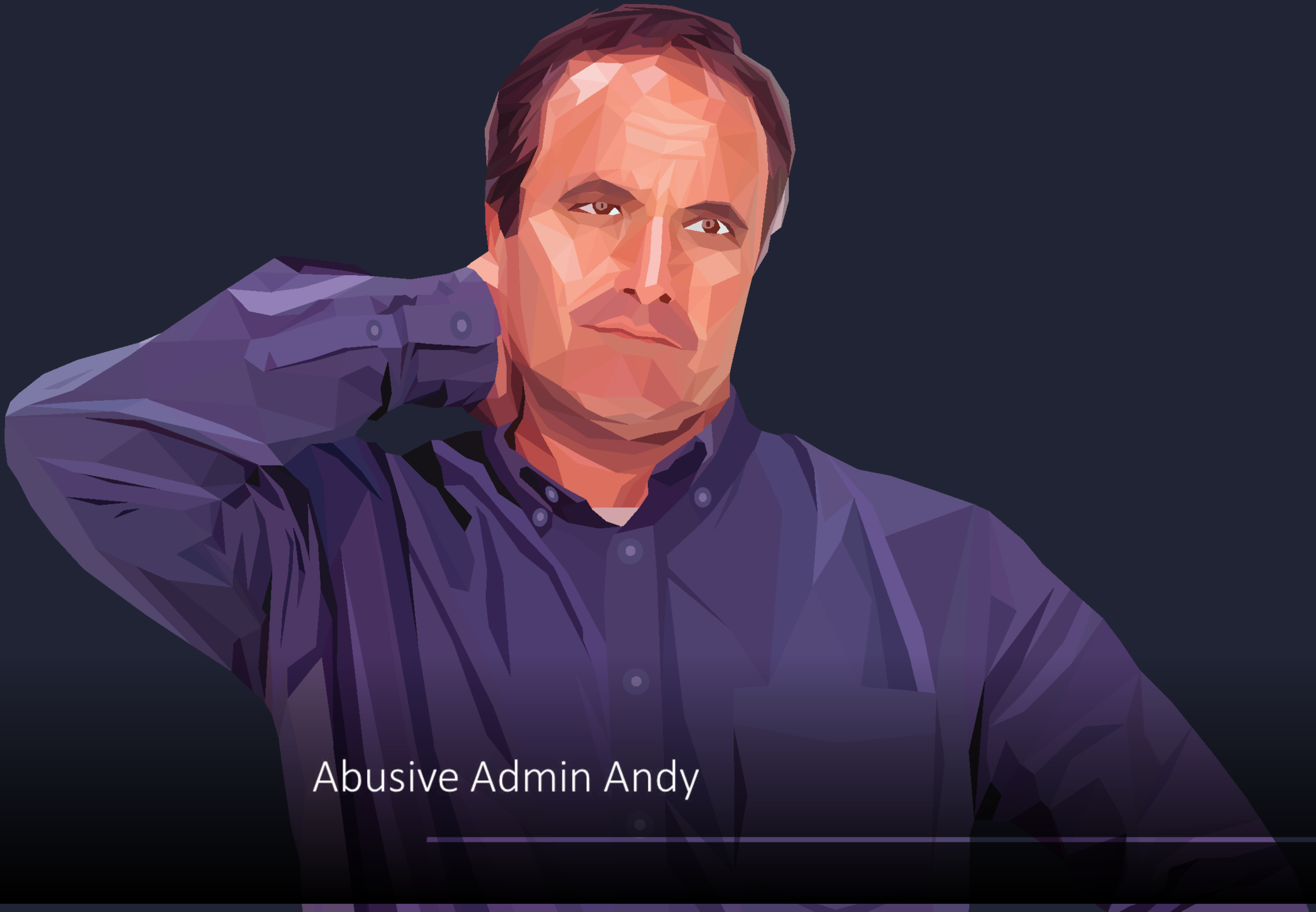
Let’s look at persona’s



The canary in the coal mine: Malware Molly

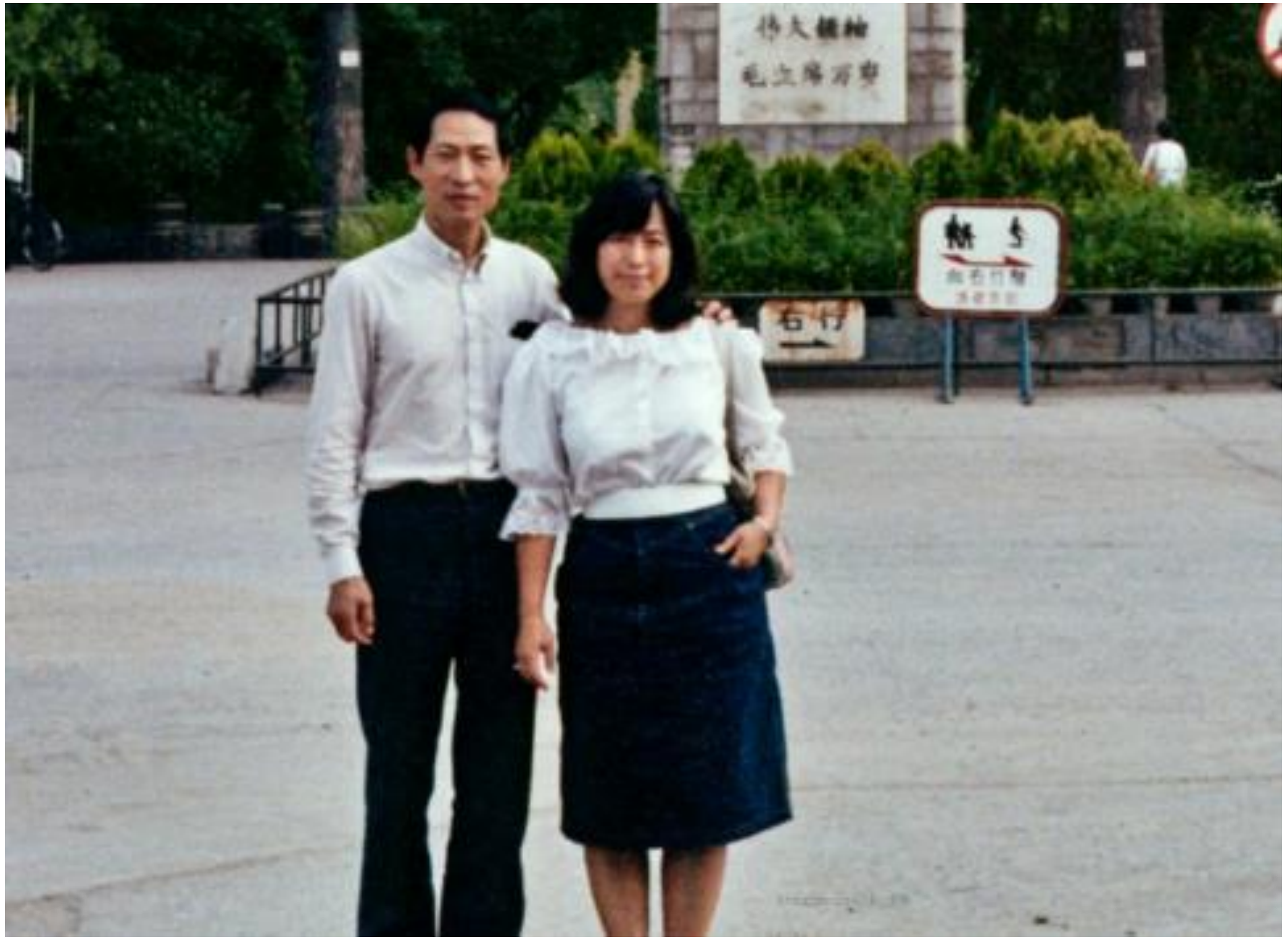


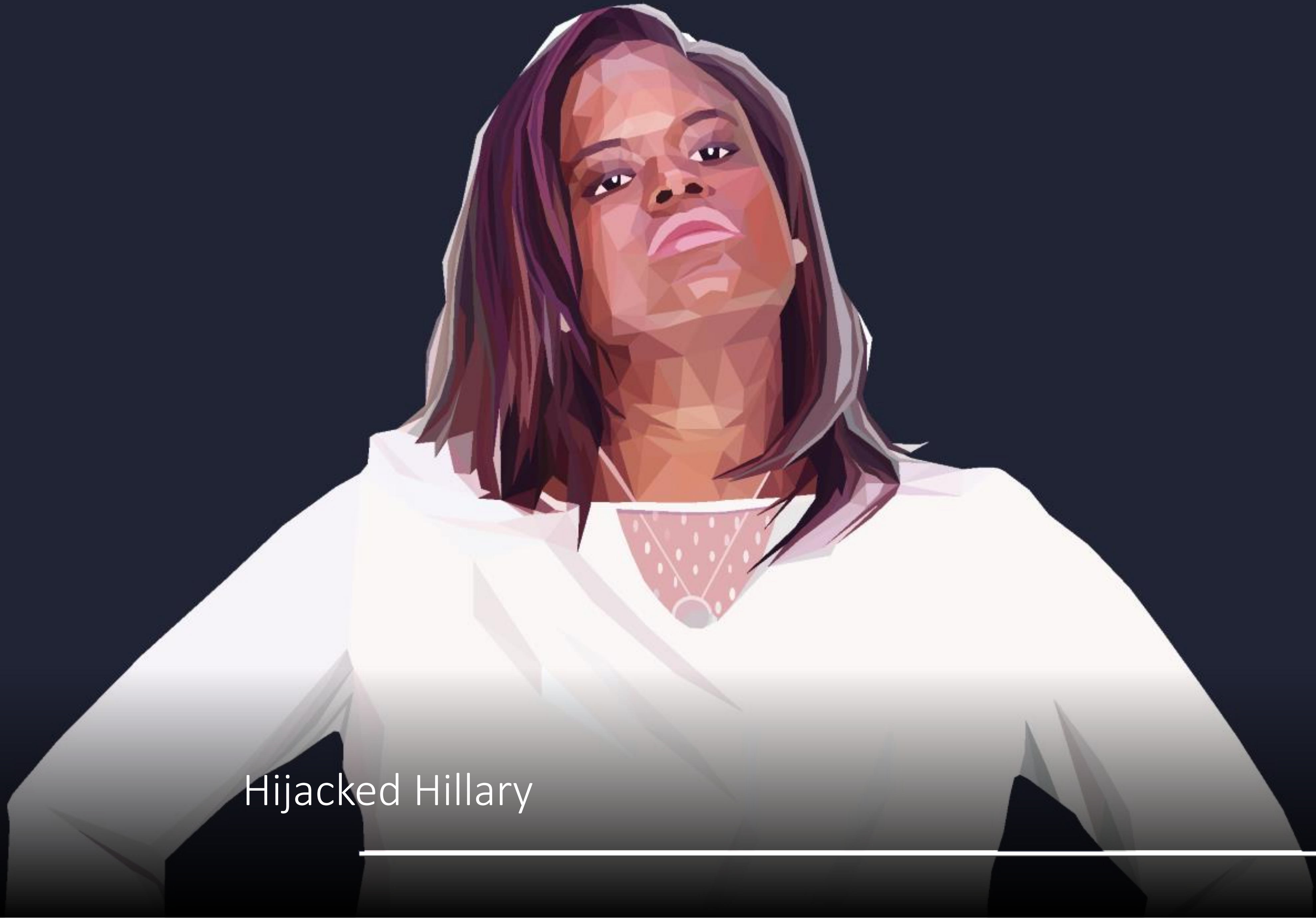
```
Your computer files have been encrypted. Your photos, videos, documents, etc....
But, don't worry! I have not deleted them, yet.
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key.
Every hour files will be deleted. Increasing in amount every time.
After 72 hours all that _
```



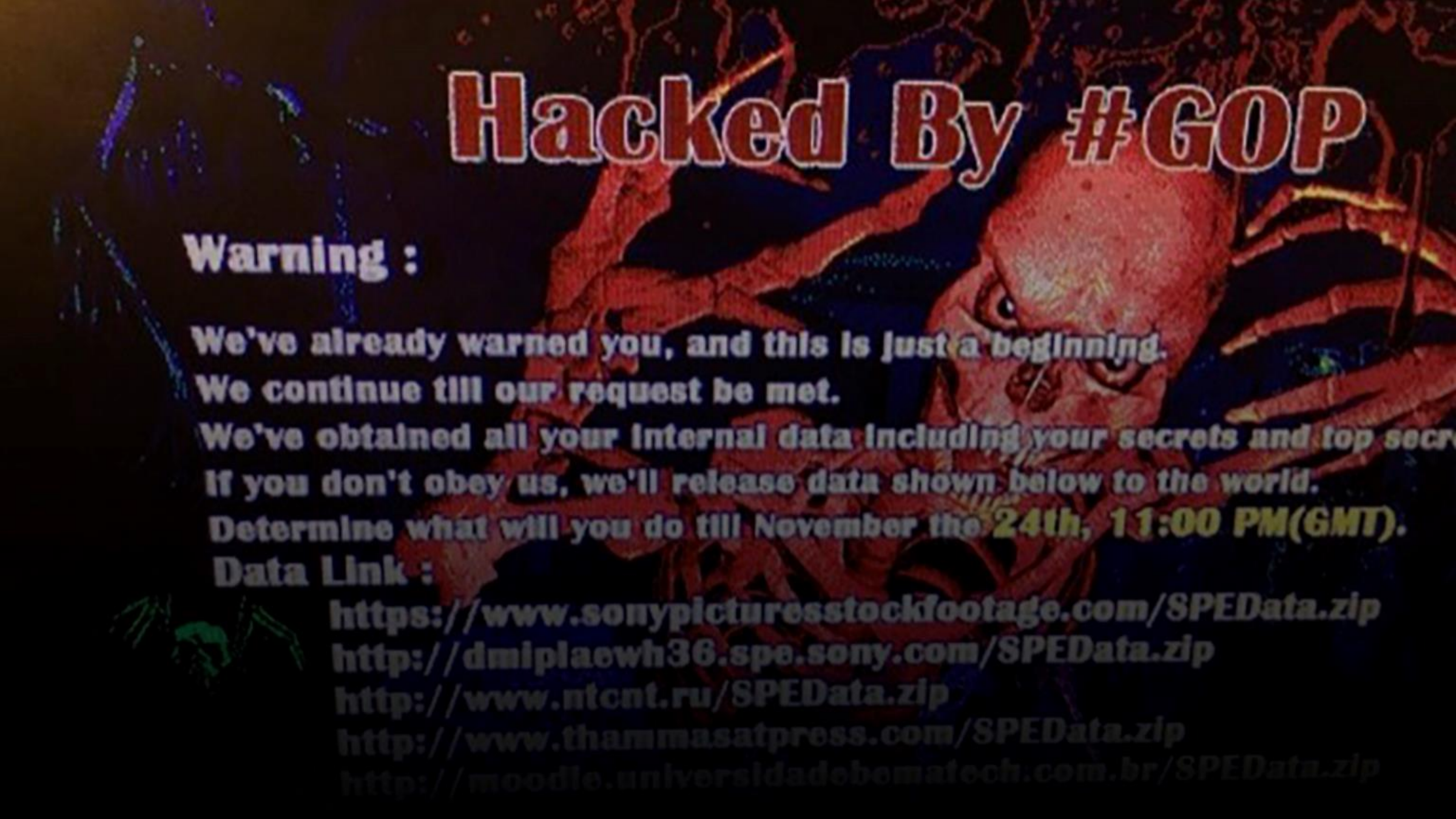
Abusive Admin Andy

Does anyone know who this is?





Hijacked Hillary



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 secr
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

Disgruntled Dan

https://www.biography.com/people/edward-snowden-21262897

Insider Threat Activities/Examples

1. Hijacked Hilary logs into VPN from North Korea at 2:15am.
2. Malware Molly opens a ransomware email and clicks on the link.
3. Admin Andy opens an exec mailbox, read’s email, marks as unread to cover his tracks.
4. Disgruntled Dan (software developer) accesses a lot of idle sensitive data.

1. Atypical GEO-location and a login time that is many deviations from normal.
2. Crypto activity detected, many files modified (encrypted) in short amount of time.
3. Access to a mailbox other than their own, marking emails as unread from a non-owner user account (obfuscation).
4. Access to data that hasn’t been access in a long time period, sensitive in nature, and it occurred in a short time frame.

Why is Ransomware so dangerous when it becomes an insider?

Insiders have a lot of access…

62%	of end users say they have access to company data they probably shouldn’t see
29%	of IT respondents say their companies fully enforce a strict least privilege model

Ponemon INSTITUTE

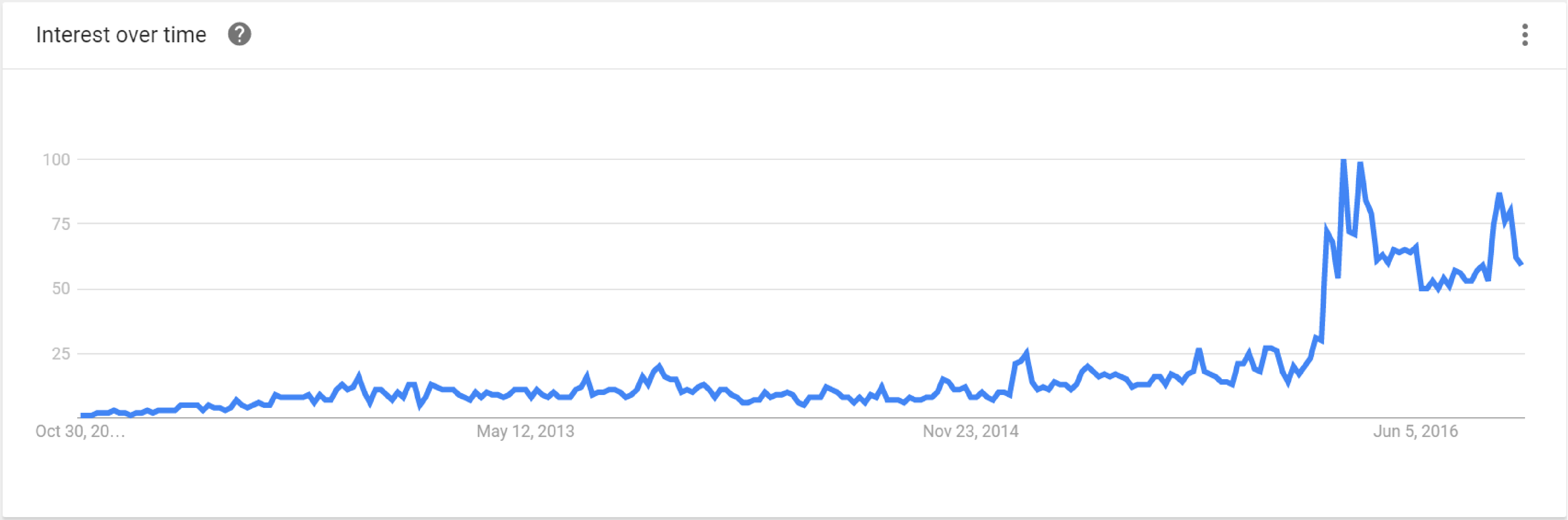
Very few watch what insiders are doing…

35%	of organizations have no searchable records of file system activity
38%	do not monitor any file and email activity.

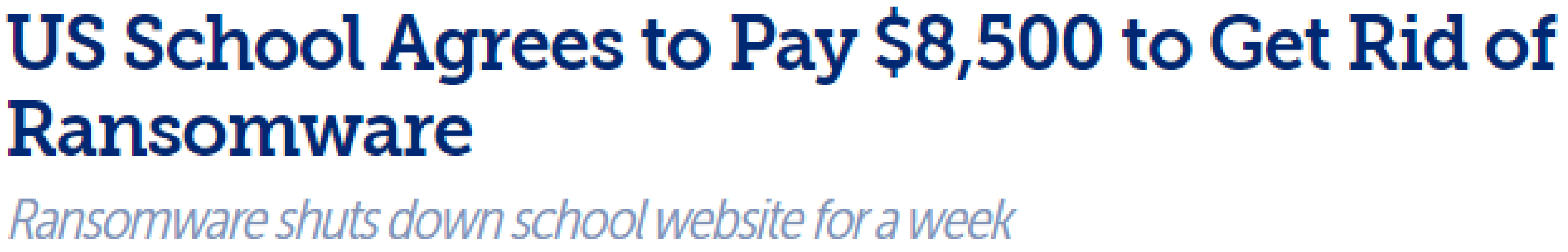
Ponemon INSTITUTE

> “I am seeing around 4,000 new infections per hour, or approximately 100,000 new infections per day.”

– Kevin Beaumont, Malware Analyst

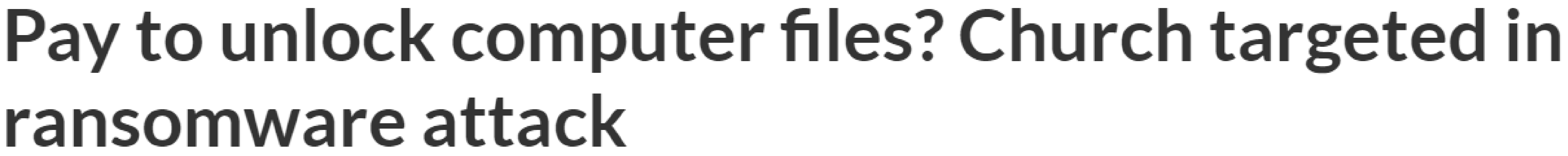


Google Trends: Ransomware

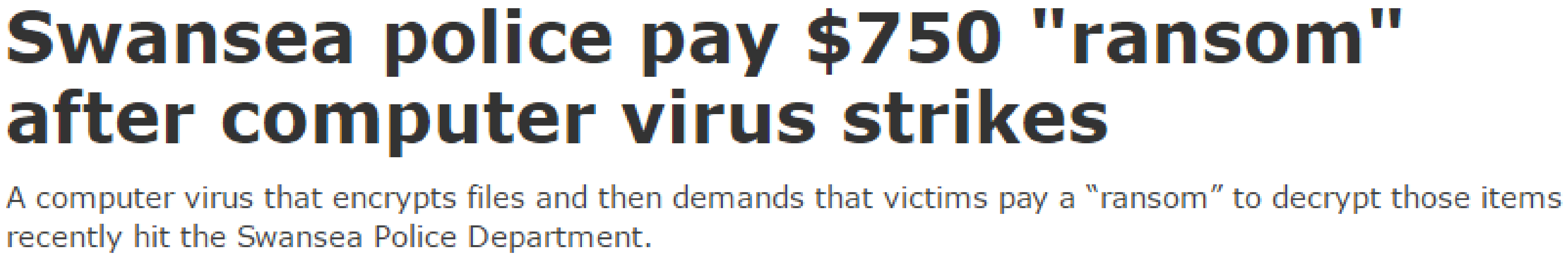


US School Agrees to Pay $8,500 to Get Rid of Ransomware

Ransomware shuts down school website for a week



Pay to unlock computer files? Church targeted in ransomware attack



Swansea police pay $750 "ransom" after computer virus strikes

A computer virus that encrypts files and then demands that victims pay a "ransom" to decrypt those items recently hit the Swansea Police Department.

But what changed?

Bitcoin: Anonymously monetizing malware at scale

Social Engineering

Hackers are finally figured out that it’s much easier to “hack a human” than it is to crack the perimeter…

Why crack the vault when I can more easily get you to open the vault???

What data is most vulnerable to insider threats and ransomware?

“Data volume is set to grow 800% over the next 5 years and 80% of it will reside as unstructured data.”

So how do we mitigate the risk?

DATA USERS

Where are we shining the light?

Treat data like dollars

What’s is this UBA I’ve heard about lately?

User (and entity) behavior analytics is bringing the science of profiling and anomaly detection based on machine learning, to security.

The practice includes :

- Automatic detection of entities (users, computers, networks)
- Establishing a baseline of normal activity for the entities
- Detecting abnormal behaviors (standard deviation)

UBA vendors use packaged analytics to discover security infractions.

Old Paradigm

- Rules-based
- Signatures Based
- Identify what’s KNOWN

New Paradigm

- Machine Learning
- Security Analytics
- Big Data
- Identify what’s UNKNOWN

Purpose Built UBA

- User & Entity Behavior Baseline
- Behavioral Peer Group Analysis
- Insider Threat Detection
- Statistical Analysis
- Lateral Movement Analysis
- Polymorphic Attack Analysis
- IP Reputation Analysis
- Reconnaissance, Botnet and C&C Analysis
- Data Exfiltration Models
- External Threat Detections
- User/Device Fingerprinting

Let’s Summarize

1. The insider threat is real and is often overlooked
2. The principal of least privilege can help mitigate the risk of an insider threat or an external threat that compromises an insider.
3. The threat of ransomware will continue to evolve primarily because human’s are susceptible and curious by nature
4. Ransomware’s evolution is highly dependent on crypto-currency
5. User Behavior Analytics is a game changer. Without it, we can’t identify unknown threats and with the ever-changing user behavior, it becomes difficult to understand what’s normal vs not normal.

Jim Kennedy
Sales Engineer
Varonis
518-221-5601
jkennedy@Varonis.com