

BIG UNIVERSITY 2018



BIG UNIVERSITY 2018

Construction Track



BIG UNIVERSITY 2018

Construction Track

SESSION 1

Office, Team and Field

Matt Redlund & Peggy McCain (Viewpoint)



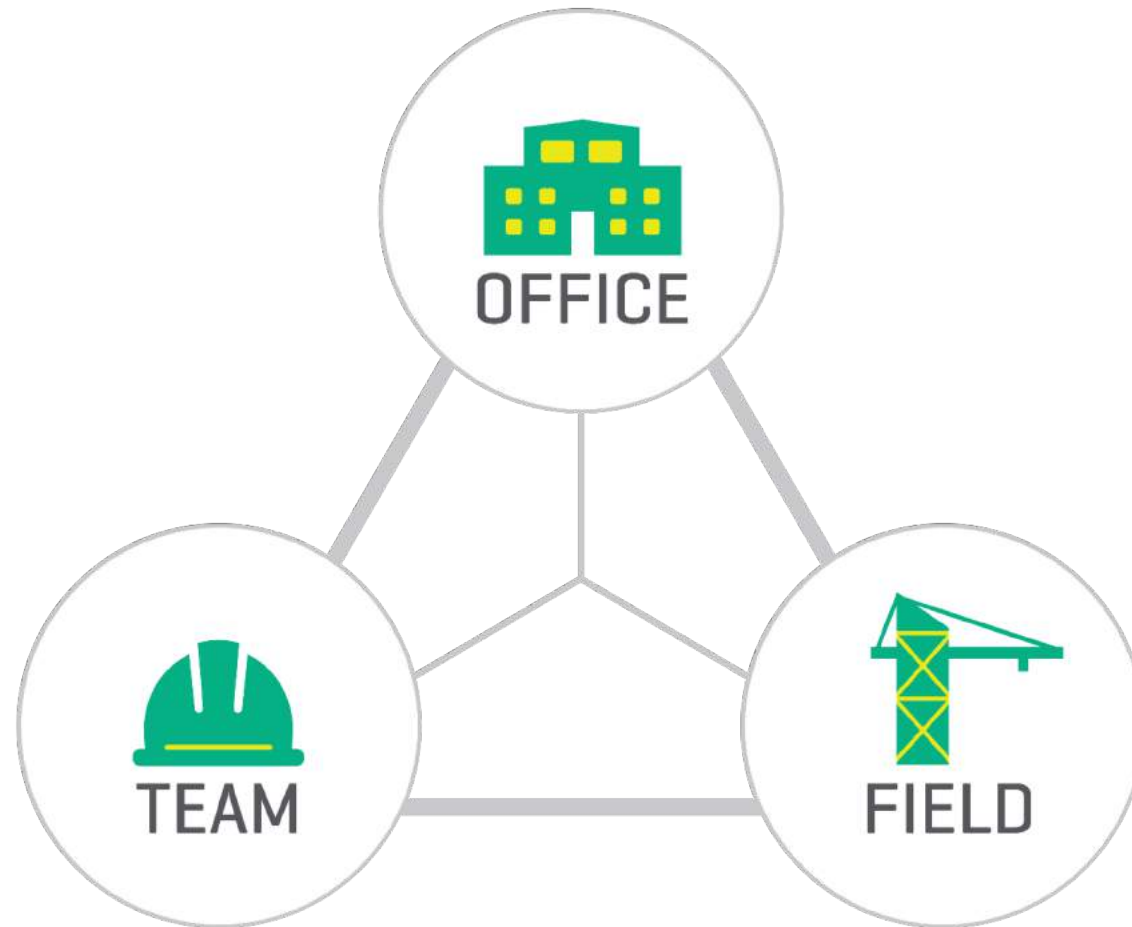
EXCITING VIEWPONT NEWS

ONE Viewpoint

- Viewpoint has entered into an acquisition agreement with Trimble
- Acquisition of Keystyle, a leading Viewpoint technology partner
- 700 employees, 200 in R&D
- 2017 User Conference- largest ever!
- 8,000 companies worldwide now use Viewpoint
- Over 70% growth in our mobile applications
- Cloud offering has exploded
- Roadmap- Focused on connecting & integrating office, team, and field

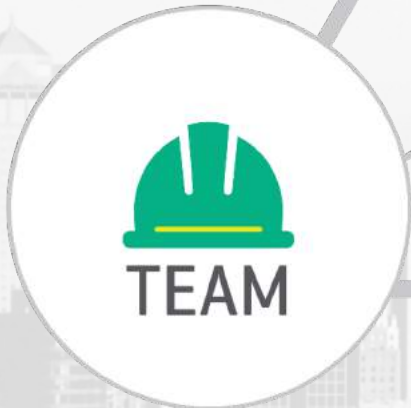


CONSTRUCTION SPANS THREE UNIQUE GROUPS



INTEGRATED SOLUTIONS FOR OFFICE, TEAM, & FIELD

 | **Team**™



 | **Vista**™

 | **Spectrum**®

 | **ProContractor**™



 | **Field View**™

 | **Field Time**™



We solve the classic “Silo” problem...

THE CLASSIC SILO SCENARIO

Multiple Programs/Silos & Nothing Connected...

- Project documents done in Excel/Word and stored all over the place
- Documents stored locally or on the “E drive”
- Timesheets done on paper, daily field reports on paper, and filing cabinets galore!



WHAT IS TEAM?

- Collaborative Project Management
- Web-based... access from anywhere!
- Unlimited licensing
- Real PM tools that drive productivity
- RFI's, Submittals, Issues, and document management
- Daily field reports



Viewpoint team project management

THERE'S A BETTER WAY....

For two decades “integrated” third-party Project Management systems have disappeared from the market.

WHY?

They failed to *truly* integrate with ERP



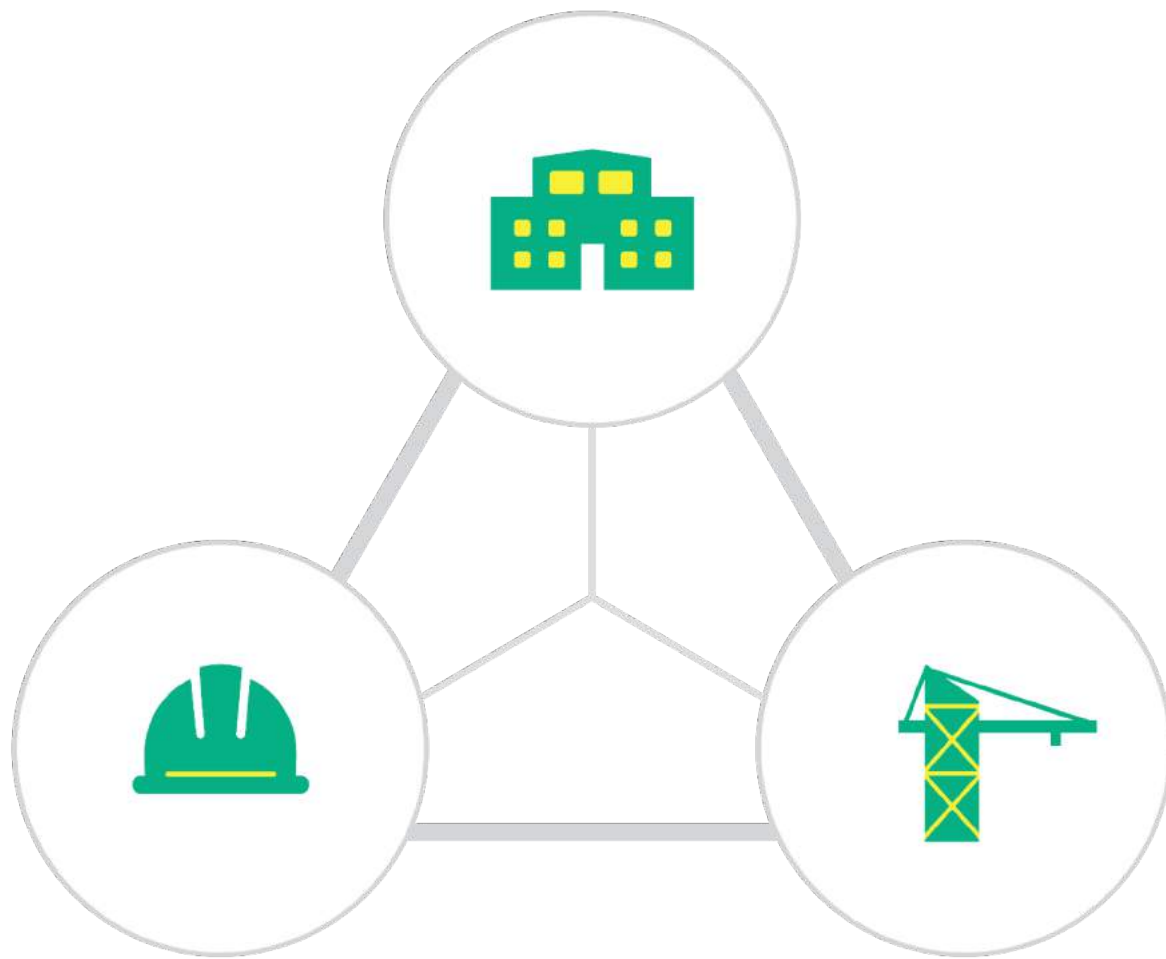
THE RIGHT TOOL FOR THE JOB



Accounting/Finance



Operations



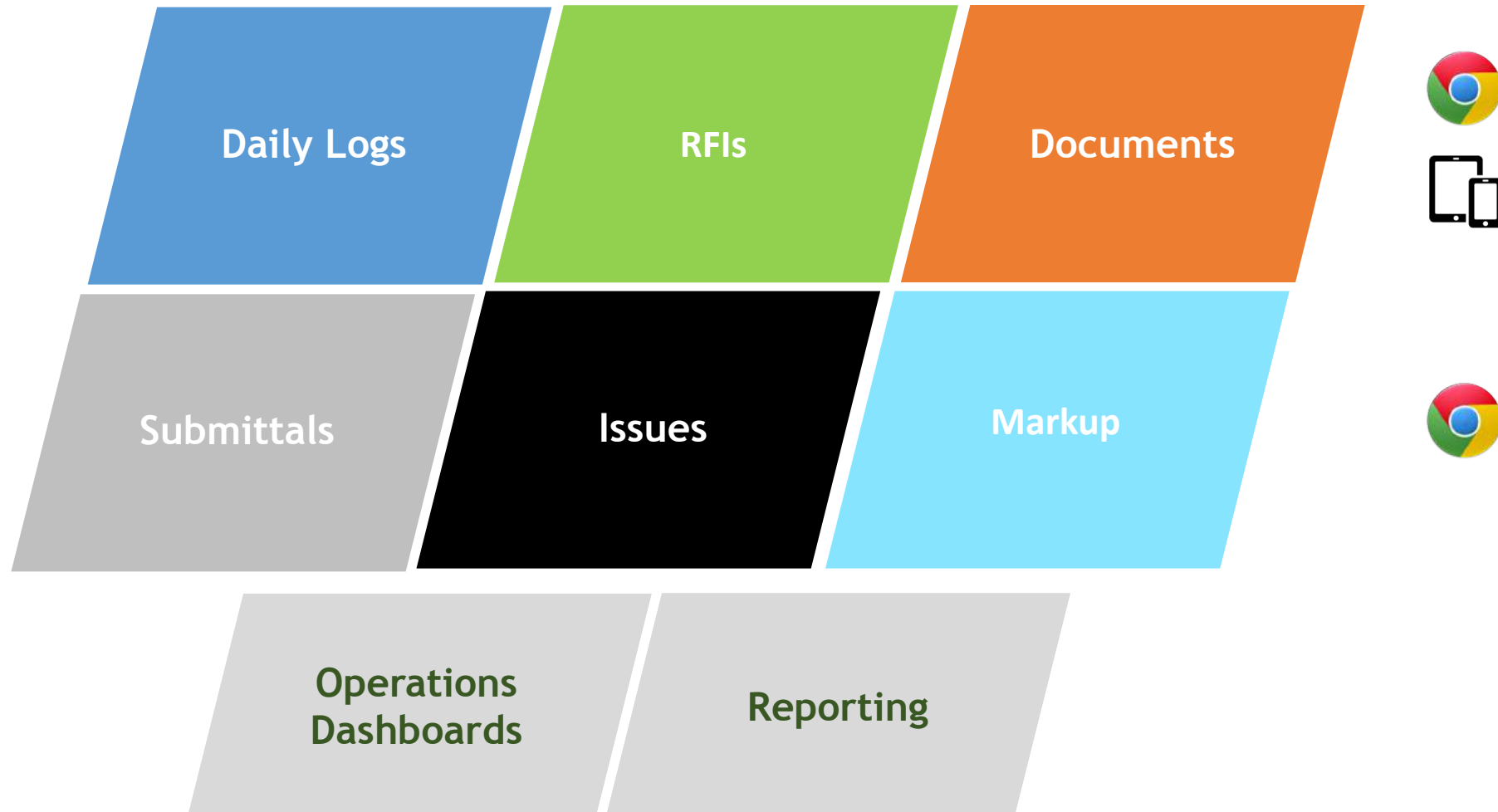
IMAGINE A
WORLD WHERE...



TEAM



PROJECT MANAGEMENT FEATURES



BUILT FROM THE GROUND UP



WHY THIS MATTERS?



Viewpoint Team helps us manage a large amount of work in a small amount of time



Bobby Asbury,
Project Manager
Leander Construction



Viewpoint was seen as customizable, flexible and easy-to-use

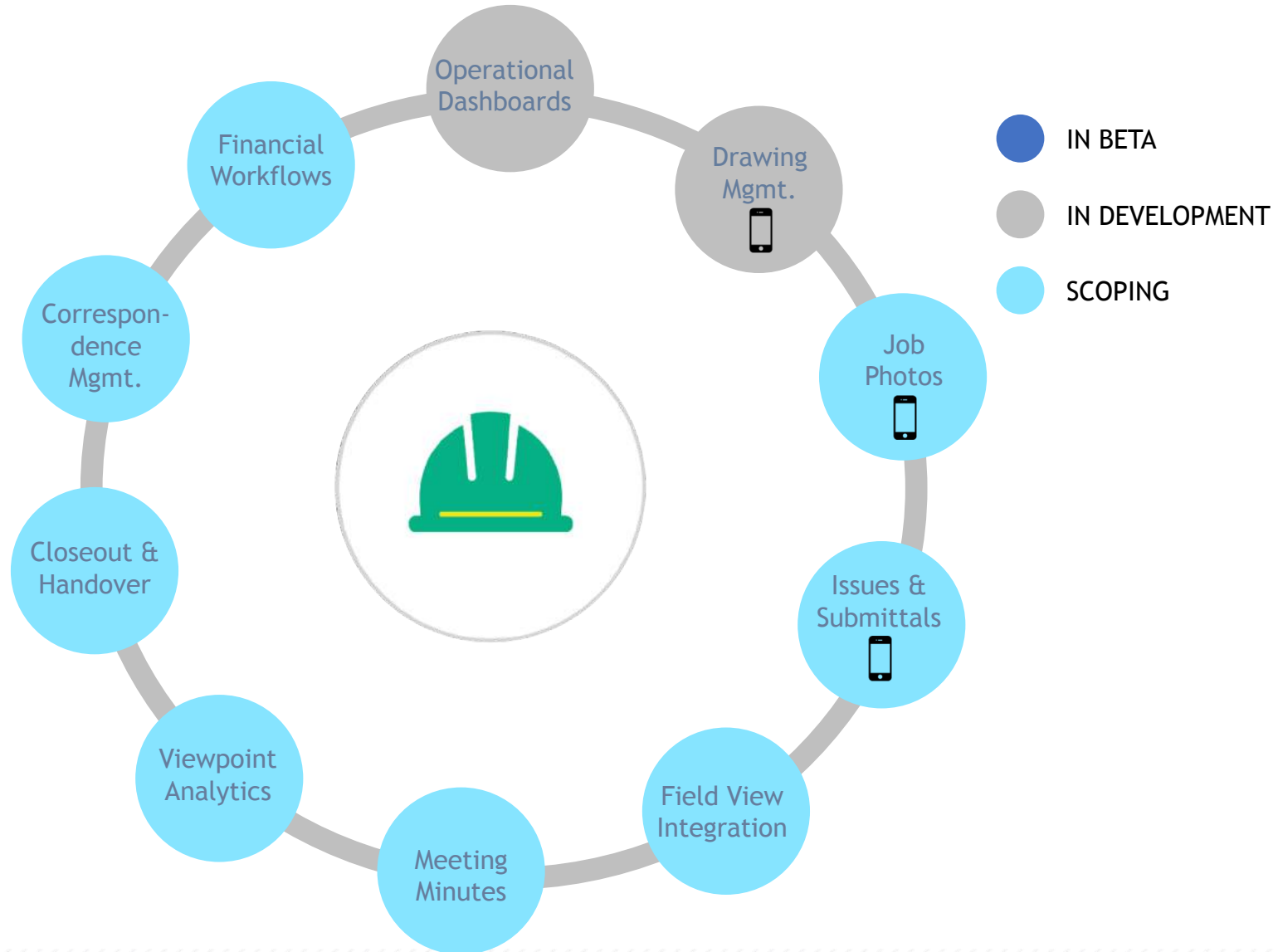


Andrea Wright,
Director of Training
Sachse Construction

The following information is intended to outline our general product direction. It is not a commitment to deliver specific features or functionality, and should not be relied upon in making decisions. The development, release, and timing of any features or functionality described for Viewpoint's products remains at the sole discretion of Viewpoint.



FEATURE ROADMAP





TEAM DEMO



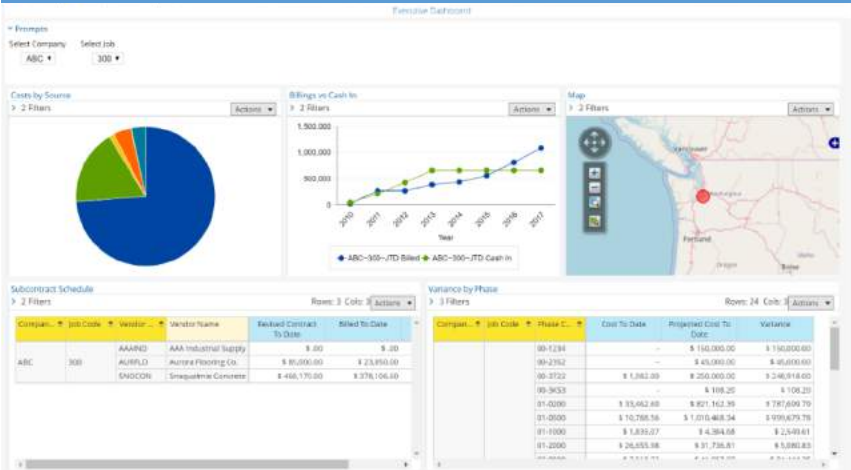
Business Intelligence & Analytics



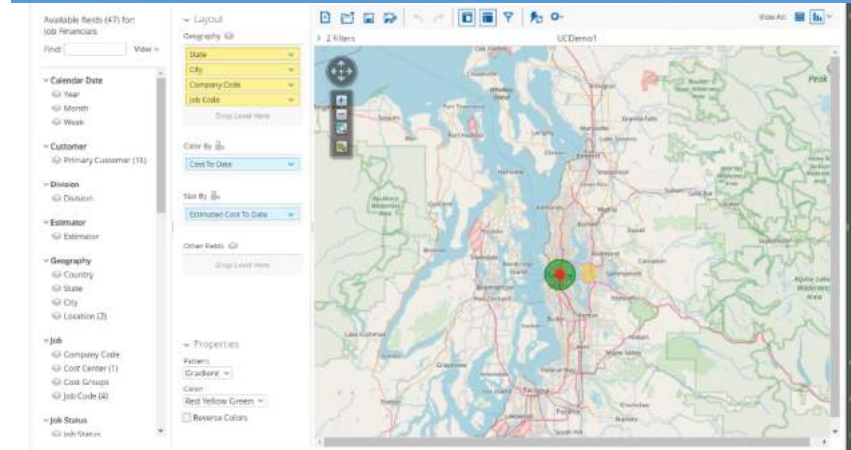
Spectrum Business Intelligence



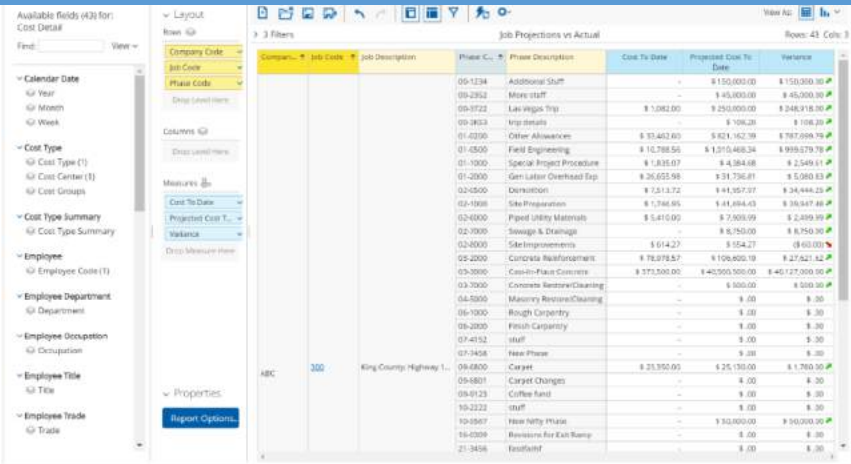
DASHBOARDS



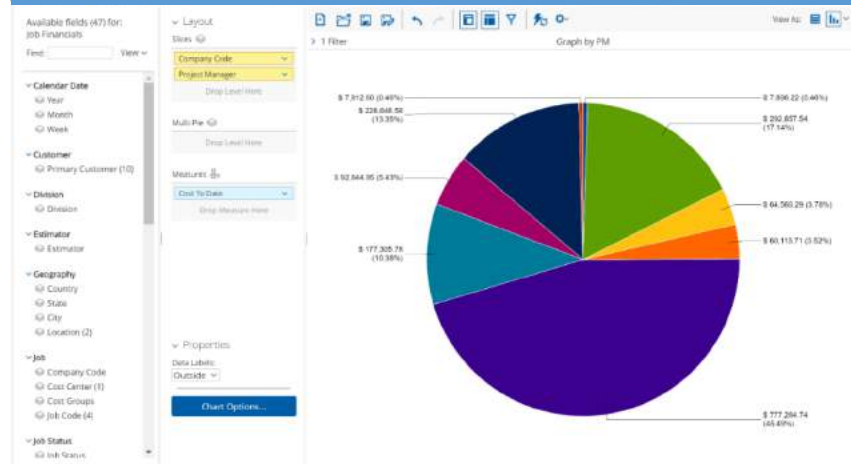
GEO MAPPING



ANALYSIS REPORTS



VISUALIZATIONS



The following information is intended to outline our general product direction. It is not a commitment to deliver specific features or functionality, and should not be relied upon in making decisions. The development, release, and timing of any features or functionality described for Viewpoint's products remains at the sole discretion of Viewpoint.

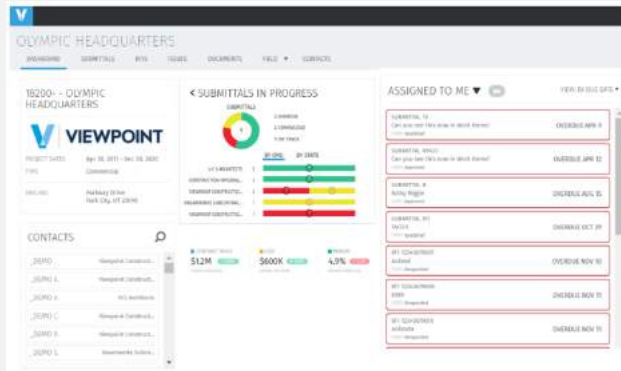


Viewpoint BI and Predictive Analytics Roadmap

Viewpoint BI and PA solutions integrate analytics capabilities with data captured by our ERP and Field collaboration tools. Our tools provide insights and actionable events to improve operational efficiencies and reduce costs

Coming Soon

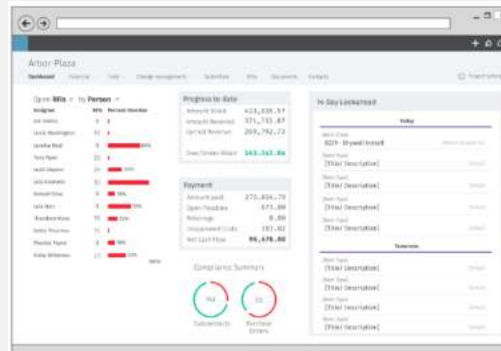
- Vista & Spectrum Job Cost data in TEAM
- Data warehouse infrastructure
- Periodic refreshes from source



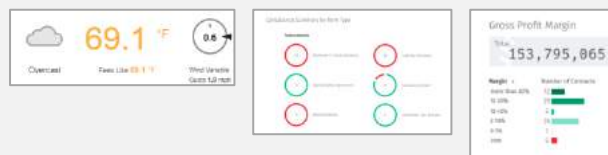
Job Cost Widget

Work In Progress

- PM Workcenters
- One place to see all your information
- Key metrics at your fingertips
- Data widgets library



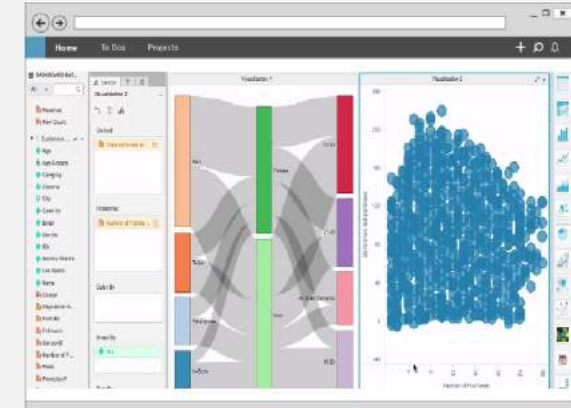
PM Workcenters



Dashboards and Widgets Library

Available Later

- Self-service reporting
- Advanced analytics platform
- Accounting, Payroll, SM/EM financials



Advanced data discovery and data visualization platform





Questions?

BIG UNIVERSITY 2018

Construction Track

SESSION 2

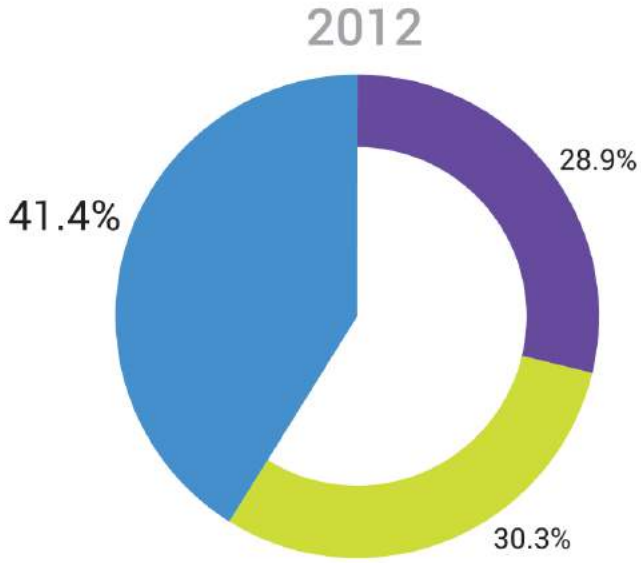
“Protecting Your Information in the Field”
Patrick Rumbaugh (Business Information Group)



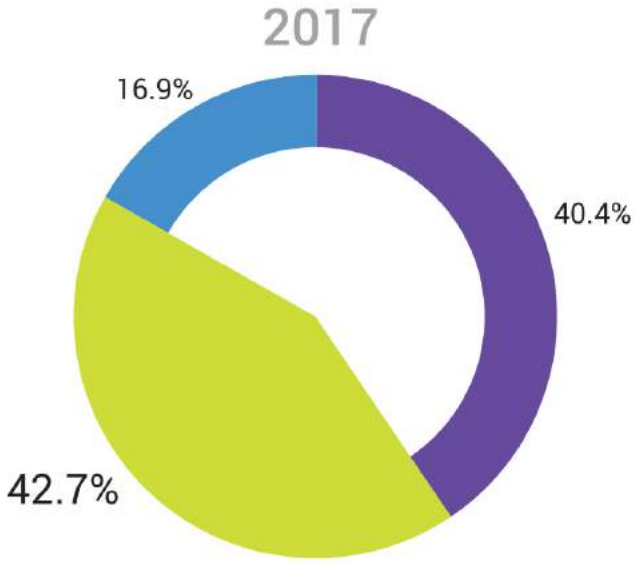
Objectives

- Explore popular technologies that are being used on jobsites
- Identify threats to be aware of
- Define better management of devices in the field

How important is technology



- Very Important
- Important
- Not Very Important



- Very Important
- Important
- Not Very Important

Technologies on the Jobsite

WHY

- Collaboration
- Accurate and timely data
- Data stored on servers that is backed up
- Create efficiencies to reduce cost
- Accurate and timely decisions

WHAT

- 3D Printing
- Augmented Reality
- BIM
- Drones
- GPS Tracking
- Laptops/Tablets/Smartphones
- Laser Scanning
- Robotics
- Virtual Reality

BENEFITS EVERYONE

- Accounting – direct integration between the office and the field
- Estimating – bringing the field to the office
- Project Management – real time data for accurate decision making
- Safety – integration, field to the office and accurate data for decision making

Threats on the Jobsite

WHAT

- Connecting to the jobsite
- Job trailers
- Out of date AV
- People
- USB devices
- Windows update

How to Better Manage the Jobsite

DEVICES ON JOBSITES



Laptop



Tablet



Smartphone



Wearable

2017

78.4%

53%

76.8%

11.1%

HOW

- Properly Securing Your Networks
- Mobile Device Management (MDM)
- Managed Services Platform
- Cloud-based Antivirus
- End User Training

Securing Your Networks

- Internal and External Networks
- What security protocols are in place to grant access company resources?
- Understand your work flows

Mobile Device Management

- Apply security login code to all devices
- Asset management
- Detect jailbroken or rooted devices
- Email password changes from centralized portal
- GPS tracking
- Logging and reporting for compliance
- Push applications to devices
- Remote wiping capability

Managed Services Monitoring Platform

- Asset tracking
- Device use
- Geolocation
- Physical health
- Proactive incident detection
- Verification of necessary services
- Windows patching and updates

Cloud-based Antivirus

- Centralized database updated by recent threats
- Only requires internet connection to get updates
- Schedule scans through portal
- Exceptions through portal
- Device and File trajectory

Security Awareness Training

- Considered proper standard of care
- Create a top down approach – no one is exempt
- Do not assume
- Emphasize the importance of data security
- Many tools to do this

Questions?

Thank you

Patrick Rumbaugh

Director of AEC Network Services

prumbaugh@businessinformationgroup.com

Business Information Group

BIG UNIVERSITY 2018

Construction Track

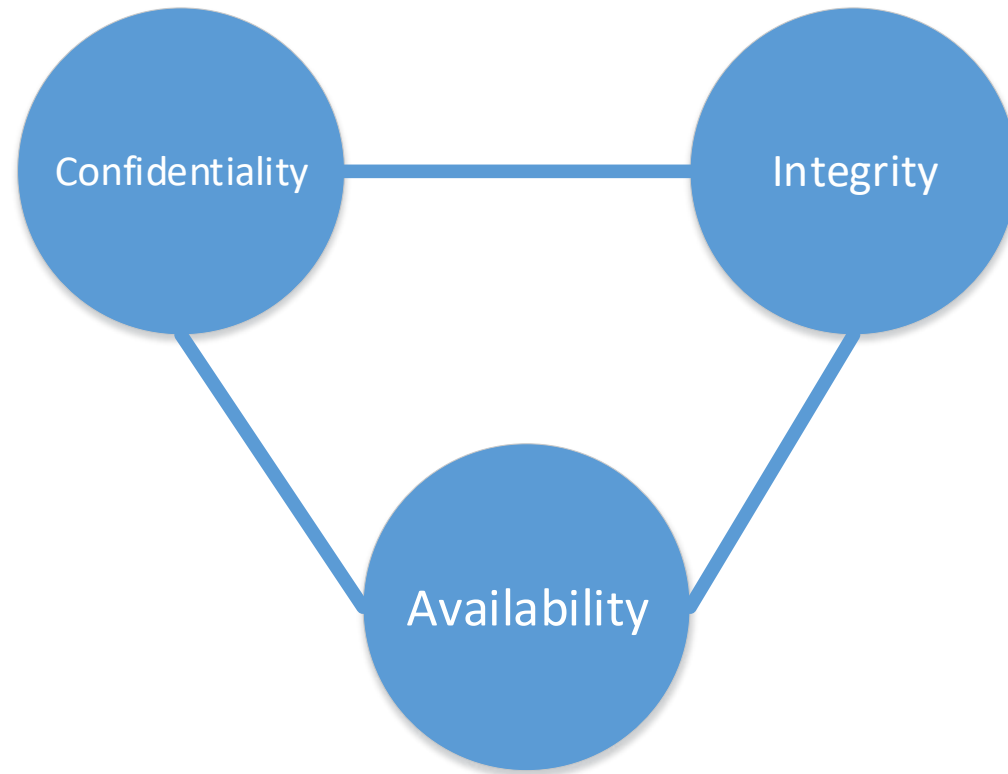
SESSION 3

How to Mitigate a Cyber Attack

Charles Getty (BIG)



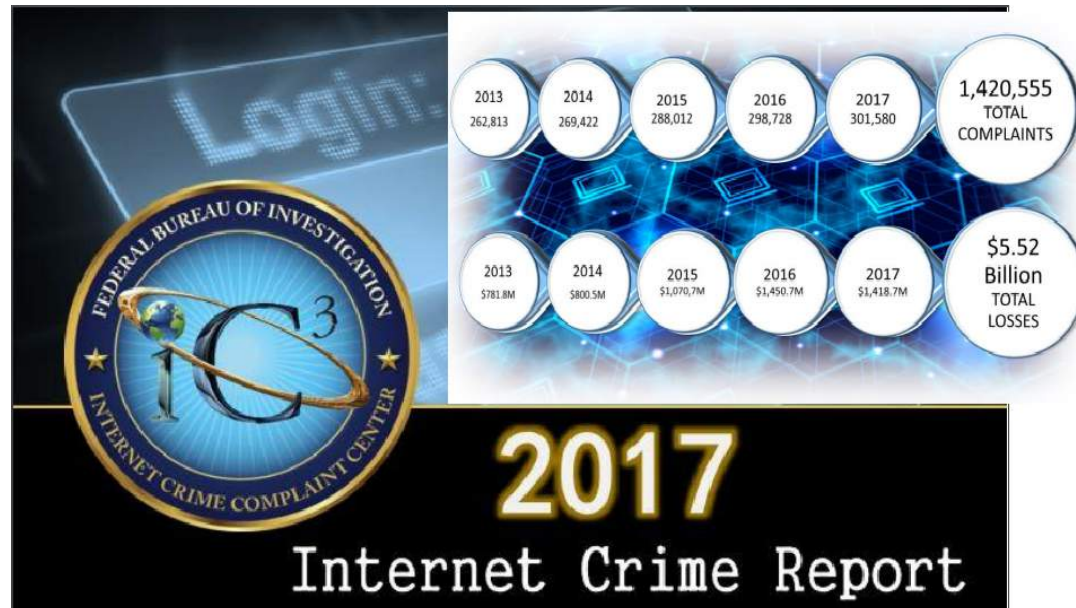
IT Security



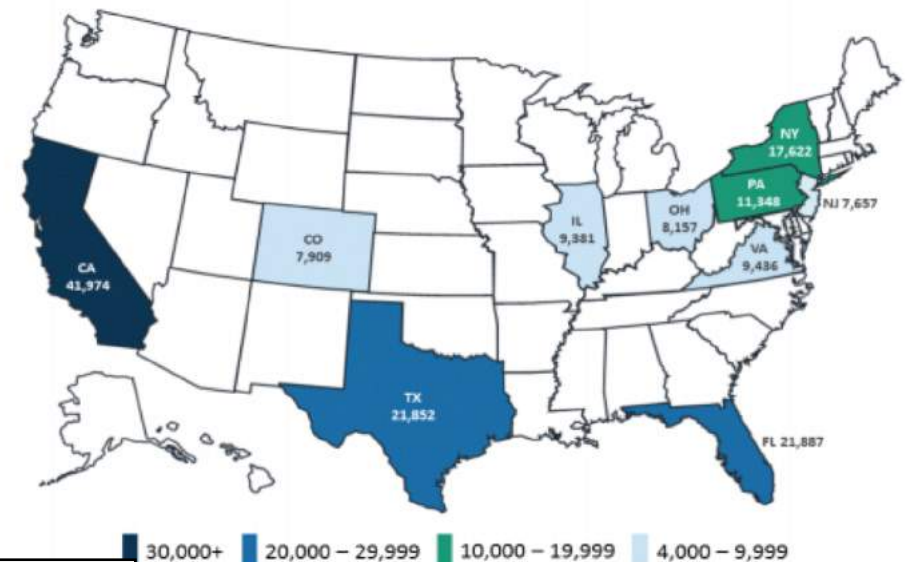
FBI Statistics

Over 5.5 Billion in losses reported over last 5 years...

Pennsylvania ranks 5th in the nation for reported incidents...



Top 10 States by Number of Victims ¹⁸



Credit: 2017 IC3 Annual Report

Agenda

- Why are you a target
- Security frameworks and strategies
- Your adversaries framework and strategy
- Walkthrough a Cyber Attack

Why are you a target?

Organized crime

- You have money
- Your customers have money
- They want money

Hacktivist

- You offend
- Your customers offend
- They want to punish

Selecting a Framework

- FISMA / NIST
- ISO 27000
- PCI/DSS
- HIPAA
- FFIEC

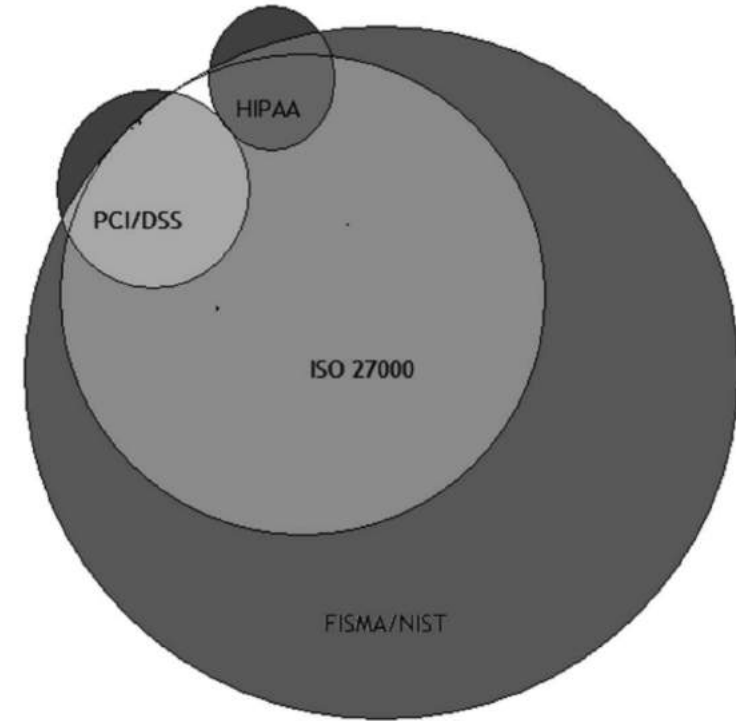


FIGURE 4 Security provisions overlap/comparison.

Credit: A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards. By: Gikas, Constantine. Information Security Journal: A Global Perspective. May2010, Vol. 19 Issue 3

NIST Framework / FISMA



Credit: N. Hanacek/NIST

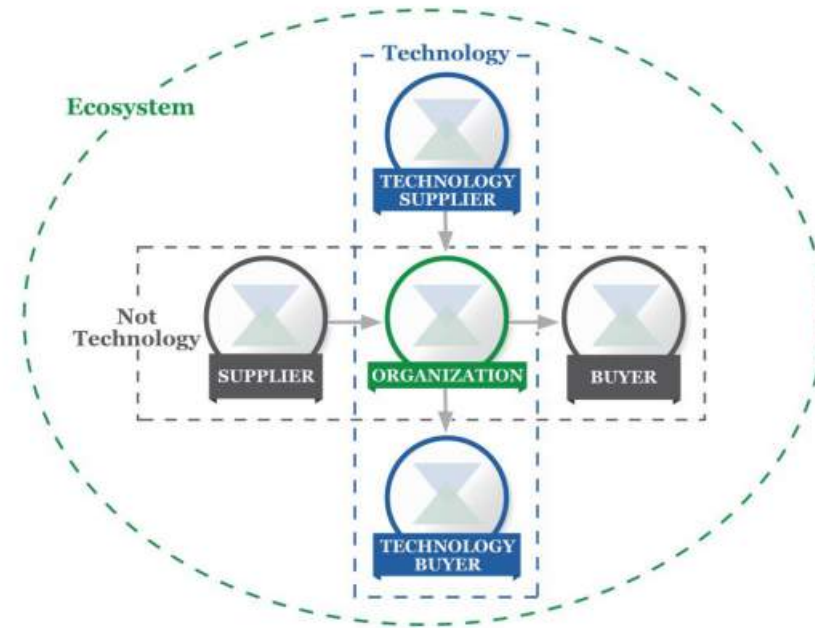


Figure 3: Cyber Supply Chain Relationships

Credit: National Institute of Standards and Technology, Cybersecurity Framework Version 1.1

Selecting Your Team

- CEO
- CISO
- CFO
- Human Resource Manager
- IT Managers
- Department Managers or Key Employees
- Lawyer
- Insurance

Implement Baseline

- Identify and Classify data
- Add controls to classified data
- Identify Systems
- Implement baseline security on systems
- Train employees
- Monitor Systems
- Use tools to test baseline

Your Adversary's Framework



Credit: Dell
SecureWorks

Searching for Vulnerable systems

Shodan

Secure | <https://www.shodan.io>

Shodan Developers Book View All...

SHODAN

Explore Developer Pricing Enterprise Access Contact Us

New to Shodan? [Login or Register](#)

The search engine for **Webcams**

Shodan is the world's first search engine for Internet-connected devices.

[Create a Free Account](#) [Getting Started](#)



Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.



See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!



Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.



Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

Acquiring Tools

- Malware as a Service
- Buy Malware on Dark Web
- Hire Hackers
- Monitor Security Blogs
- Steal code from Proof of Concepts
- Reverse Engineer Patches



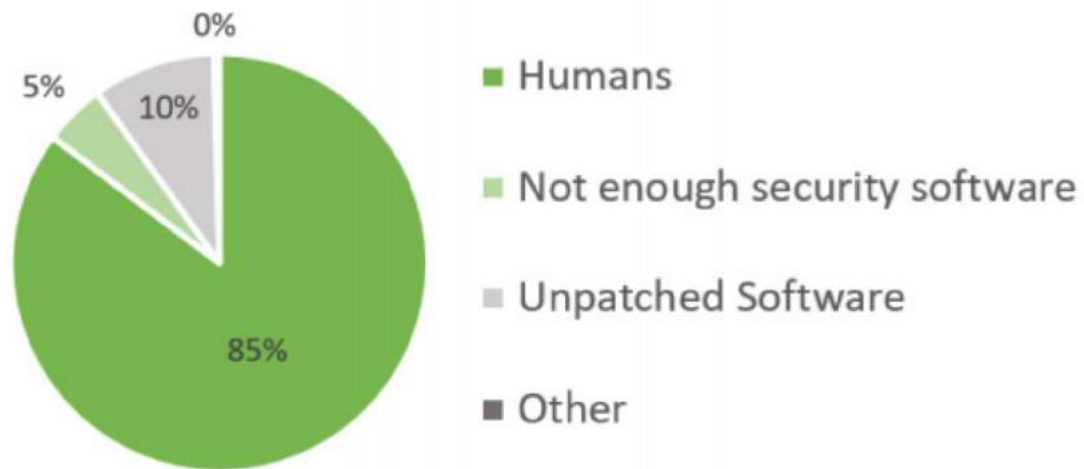
Research

- Company Web site
- LinkedIn
- Facebook
- Google
- Press Releases
- Vendor Websites



BlackHat Survey

- Cause of Compromise

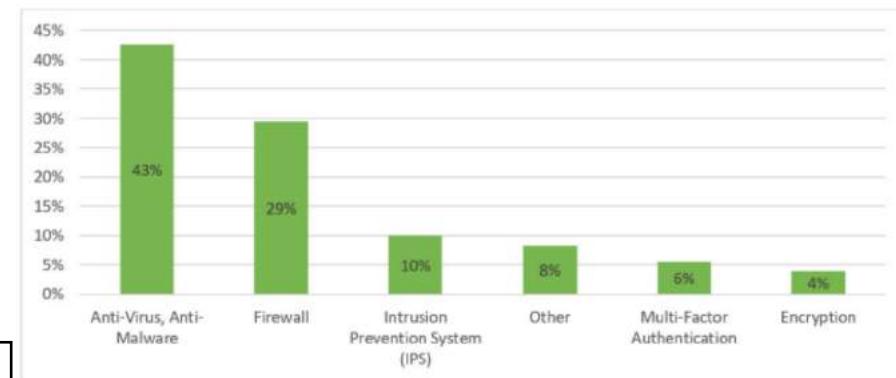


Credit: 2017 Black Hat Attendee Survey, Thycotic

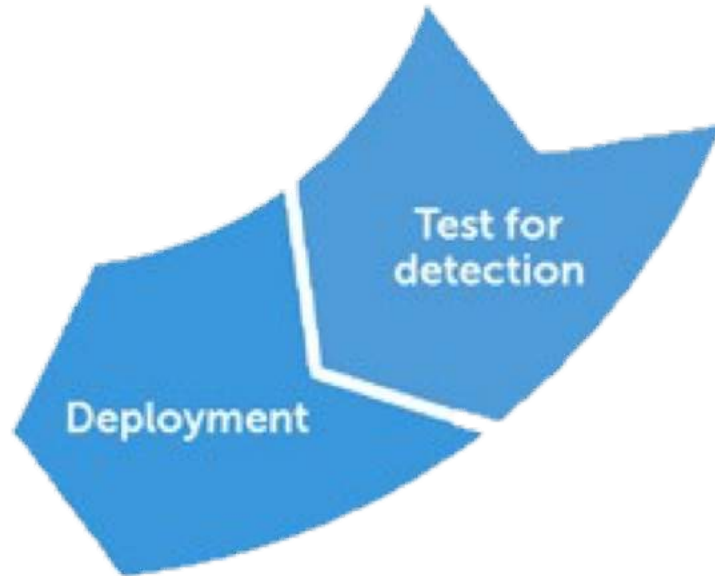
73% say traditional perimeter security firewalls and antivirus are irrelevant or obsolete

The focus on hacking privileged and email accounts reflects a recognition on the part of hackers that traditional perimeter security is no longer a barrier to getting inside networks and gaining access to critical data.

Anti-virus and anti-malware are considered the “least effective and easiest to get past” security technologies by 43% of the Black Hat survey respondents, followed by 30% of Black Hat respondents naming firewalls the easiest security technology to get past.



Test and deploy




- Phishing
- Spear Phishing
- Whaling
- Vishing
- LinkedIn
- Facebook
- Unpatched Systems (VPN, Web, Cameras, HVAC, etc....)

Phishing Counter Measures

- Web Filtering
- Email Filtering
- Advanced Malware Protection
- Sandboxing and SafeLinks
- Training

Social Engineering Red Flags



The diagram shows an email interface with several red flags pointing to specific elements:

- FROM:** Points to the sender's email address: "YourCEO@yourorganization.com".
- DATE:** Points to the date: "Monday December 12, 2016 3:00 AM".
- SUBJECT:** Points to the subject line: "My money got stolen".
- ATTACHMENTS:** Points to a document icon in the email body.
- CONTENT:** Points to the main body text of the email.
- TO:** Points to the recipient's email address: "You@yourorganization.com".
- HYPERLINKS:** Points to a URL: "http://www.bankofamerica.com".

FROM

- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from someone **outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like `microsoft-support.com`)?
- I don't **know the sender personally** and they were **not vouched for** by someone I trust.
- I don't have a **business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink** or an **attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a big red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, `www.bankofamerica.com` — the "m" is really two characters — "r" and "n."

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant or does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that I was **not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on** is a `.txt` file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar or spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd or illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

© 2017 KnowBe4, LLC. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

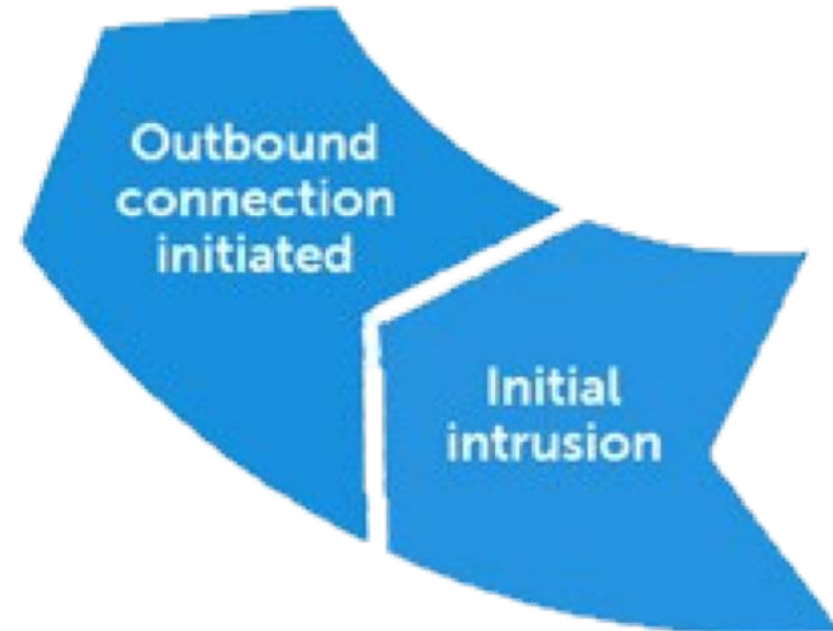
Credit: Knowbe4

Anything you can do they can do and more...

- Weigh the convenience of anywhere access against the cost of adequately securing it.
- Research systems vulnerability history (no history is a red flag)
- Change Default passwords
- Use secure passphrase
- Patch quickly, Patch often

Initial Intrusion

- Test outgoing connections
- Setup Command & Control
- Sophisticated attack – sleep
- Smash and Grab – Harvest saved passwords and credit cards... encrypt drive and demand ransom



Counter Measures

- Firewall rules
- Intrusion Protection System (IPS)
- Network Based Advanced Malware Protection (AMP)
- AntiVirus / AntiMalware
- Connection Logging and Analysis
- Security Information and Event Management (SIEM) Systems
- Patch Management



Expand Access and Obtain Credentials



- Elevate privileges
- Harvest Email Address Book
- Harvest Saved Passwords
- Harvest Cookies
- Network Scanning / NMAP
- Scan Files for Credentials
- Send phishing emails as user

Counter measures

- Patch Management (Applications too... not just OS)
- Anti-Virus / Anti-Malware
- Intrusion Protection Systems (IPS)
- Vulnerability scanning / auditing
- Multi-factor Authentication (MFA)
- Identity Management Systems
- Encryption
- Training
- Honeypots, Honeynets, Honeyclients, and Tarpits (use extreme caution)

Strengthen Foothold

- Use Harvested data
- Deploy Malware and RATs to additional machines
- MAC flooding
- ARP Poisoning
- Network Scanning
- Switch Spoofing
- DNS Poisoning
- DHCP Server Spoofing



Counter Measures

- Port Security
- ARP Inspection
- Network Monitoring
- SIEM Systems
- IPS
- Open DNS / Cisco Umbrella
- DHCP Snooping
- Rogue Server Detection
- Honeypots, Honeynets, Honeyclients, and Tarpits

Exfiltrate Data



- Upload valuable data
- Upload credentials
- Upload cookies
- Install Crypto Miners

Counter Measures

- Data Encryption
- Data Loss Prevention Systems
- Web Filtering
- Advanced Malware Protection
- Cyber Insurance

Cover Tracks

- Delete or overwrite logs
- Sleep RATs
- Divert attention with malware
- ... Choose new targets



Counter Measures

- Centralized Logging
- IPS
- Advanced Malware Protection
- Forensics

Stacking the deck

- Choose a framework
- Start with baseline (best practices)
- Stack your defenses in depth
- Test your defenses
- Stay informed
- Evolve your defenses (next practices)
- Plan for the worst
- Test your response plan

Questions?

Thank you

Charles Getty

Senior Network Architect

cgetty@businessinformationgroup.com

Business Information Group