PROVIDENCE BUSINESS NEWS

PBN SUMMIT CYBERSECURITY

October 11, 2018

#PBNCYBER SUMMIT

PROVIDENCE BUSINESS NEWS
PBN
SUMMIT
CYBERSECURITY

PRESENTING SPONSOR

BlumShapiro

Accounting | Tax | Business Consulting

#PBNCYBER SUMMIT

PROVIDENCE BUSINESS NEWS
PBN
SUMMIT
CYBERSECURITY

PRESENTING SPONSOR

PARTRIDGE
SNOW &
HAHN LLP

#PBNCYBER SUMMIT

PROVIDENCE BUSINESS NEWS
PBN
SUMMIT
CYBERSECURITY

PARTNER SPONSOR

BRYANT UNIVERSITY
1863

Bryant University
Executive Development Center

#PBNCYBER SUMMIT

PARTNER SPONSOR

COX
Business®

PARTNER SPONSOR

MARSH & McLENNAN
AGENCY

PARTNER SPONSOR

SecureFuture
TECH SOLUTIONS

Proactive Today for a Brighter Tomorrow

PROVIDENCE BUSINESS NEWS
PBN SUMMIT
CYBERSECURITY

PARTNER SPONSOR

Webster Bank

#PBNCYBER SUMMIT

PROVIDENCE BUSINESS NEWS

PBN SUMMIT CYBERSECURITY

October 11, 2018

#PBNCYBER SUMMIT

PROVIDENCE BUSINESS NEWS
PBN SUMMIT
CYBERSECURITY

PANEL 1

Jeffrey Ziplow
Cybersecurity Risk Assessment Partner
BlumShapiro

Francesca Spidalieri
Senior Fellow, Cyber Leadership
The Pell Center, Salve Regina

Jason Farmer
Senior Solution Manager
RiskSense

Wade Chmielinski
AVP, Cyber Security Consultant
FM Global

#PBNCYBER SUMMIT

PROVIDENCE BUSINESS NEWS PBN SUMMIT CYBERSECURITY

Jeffrey Ziplow

Cybersecurity Risk Assessment Partner

BlumShapiro

Accounting | Tax Business Consulting

#PBNCYBER SUMMIT

Francesca Spidalieri

Senior Fellow,
Cyber Leadership

SALVE REGINA UNIVERSITY

PELL CENTER
for INTERNATIONAL RELATIONS
and PUBLIC POLICY

Jason Farmer

Senior Solution Manager

RiSKSENSE®

#PBNCYBER SUMMIT

Wade Chmielinski

AVP, Cyber Security Consultant

FM Global®

#PBNCYBER SUMMIT

PANEL 1

Jeffrey Ziplow
Cybersecurity Risk Assessment Partner
BlumShapiro

Francesca Spidalieri
Senior Fellow, Cyber Leadership
The Pell Center, Salve Regina

Jason Farmer
Senior Solution Manager
RiskSense

Wade Chmielinski
AVP, Cyber Security Consultant
FM Global

PBN CYBERSECURITY SUMMIT

Francesca Spidalieri

Senior Fellow for Cyber Leadership
Pell Center
Salve Regina University

@Francesca_cyber

11 October 2018

PELL CENTER
for INTERNATIONAL RELATIONS
and PUBLIC POLICY

#PBNCYBER SUMMIT

TRENDS & THREATS IN 2018

- **Increased Awareness**
- **Increased Dependencies**
- **Increased Vulnerabilities**
- **Increased Costs** of data breaches and cyber disruptions:
  - Cybercrime costs the global economy as much as **$600 billion** annually;
  - The average organization takes **~197 days** to identify that an incident has occurred and **69 days** to contain it – the longer it takes, the higher the costs;
  - The average cost of a data breach in the US is **~$7.9 million**.
- Most organizations are still in a **reactive mode** – large companies to SMBs to federal and state agencies.

PELL CENTER
for INTERNATIONAL RELATIONS
and PUBLIC POLICY

#PBNCYBER SUMMIT

☑ IDENTIFY & MAP YOUR SENSITIVE AND HIGH-VALUE DATA

Take stock of your most sensitive information, and determine where it is stored, where it is going, who has access to it, and how it is being protected.

What type of data?	Where is it stored?	Who has access to it?	What's the value to the organization?	Is it encrypted?	Where does it go?
		?	$ $$ $$$ $$$$ $$$$$	Yes No	

SALVE REGINA UNIVERSITY
PELL CENTER
for INTERNATIONAL RELATIONS
and PUBLIC POLICY

#PBNCYBER SUMMIT

PROACTIVE MEASURES TO DETER CYBER THREATS

- MINIMIZE the risks of an attack
- MONITOR for dangers
- MANAGE the damage

PELL CENTER
for INTERNATIONAL RELATIONS
and PUBLIC POLICY

#PBNCYBER SUMMIT

MINIMIZE: ENTERPRISE-WIDE PRIVACY + SECURITY PROGRAM

- Properly configure **firewalls** and choose **strong passwords;**
- Install and enable **encryption** on all sensitive data;
- Regularly **backup** all important information;
- Disable and do not install or use file sharing applications;
- Regularly **update antivirus** and antispyware software;
- **Audit** and assess periodically;
- **Patch** systems and conduct **penetration tests** to find vulnerabilities;

- Establish **policies**, **procedures and standards** to protect data, and determine applicable state and/or federal laws related to the same;
- Implementing security policies and processes to protect the storage and transmission of data – hold your third-party vendors accountable and expect the same high-level standards;
- Establish Website Privacy Policy and Terms of Use; Privacy Policy + Procedures; and Security Policy + Procedures;
- Educate employees through training and awareness.

PELL CENTER
for INTERNATIONAL RELATIONS
and PUBLIC POLICY

#PBNCYBER SUMMIT

MONITOR: CONSIDER THE RISKS TO YOUR DATA

Cyber Attacks: How does this happen?

- Through your network
  - Vulnerabilities in your hardware, software or systems.
  - Your employees and mistakes they might make.
  - Your clients, if, and to the extent they have access to your network.
  - Vendors and contractors, if and to the extent they have access to your network.

Threat Vectors:

- **Phishing**: A malicious "spam-like" message sent in large batches to a broad audience.
- **Spear-Phishing:** A form of phishing – messages appear to come from a familiar or trusted sender and target recipients.
- **Ransomware:** A type of malicious software designed to block access to a computer system until a sum of money is paid.

PELL CENTER
for INTERNATIONAL RELATIONS
and PUBLIC POLICY

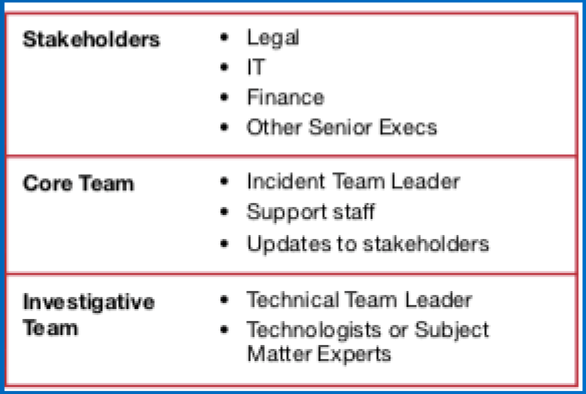
#PBNCYBER SUMMIT

MANAGE: DEVELOP AN INCIDENT RESPONSE PLAN

- Create an Incident Response and Breach Notification Plan <u>BEFORE</u> an incident occurs:
  - To be effective, the incident response plan and breach notification process should be part of a comprehensive information security program:
    - Risk assessment;
    - Trigger events;
    - Mitigation plan.

- Identify Laws and Requirements that may apply to you (e.g., GDPR);
- Communications/Media Team/Vendors in Place;
- Assemble an incident response team and assign overall responsibility for enterprise-wide information privacy & security oversight (appoint a data privacy and a data security officers).
- Make employees aware of the important role they play in privacy and security – your employees are your front line of defense when it comes to security (and also one of your highest risks).

Cyber Incident Response Team



Stakeholders	• Legal • IT • Finance • Other Senior Execs
Core Team	• Incident Team Leader • Support staff • Updates to stakeholders
Investigative Team	• Technical Team Leader • Technologists or Subject Matter Experts

PELL CENTER
for INTERNATIONAL RELATIONS
and PUBLIC POLICY

"An once of prevention is worth a pound of cure" - Benjamin Franklin

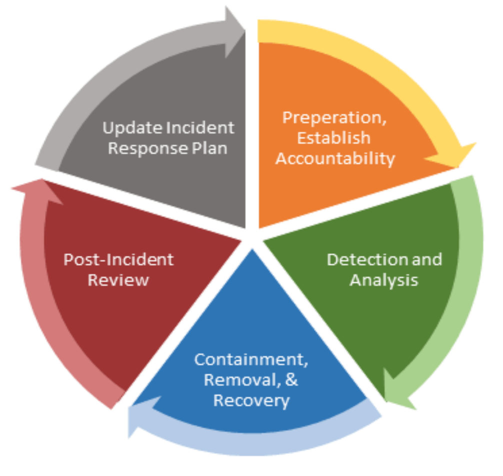
#PBNCYBER SUMMIT

MANAGE: Implement Your Incident Response Plan

✓ Prepare and define roles & responsibilities → Preparation, Establish Accountability

✓ Know how to identify/verify that an incident has occurred and what data has been compromised → Identification / Detection & Analysis

- Mitigate damages and remove threat → Containment and Removal
- Determine legal implications → Notification
- Activate your Business Continuity Plan → Recovery
- Document data breaches and all actions taken in response
- Conduct a Post-Incident Review


Update Incident Response Plan
Preperation, Establish Accountability
Detection and Analysis
Containment, Removal, & Recovery
Post-Incident Review

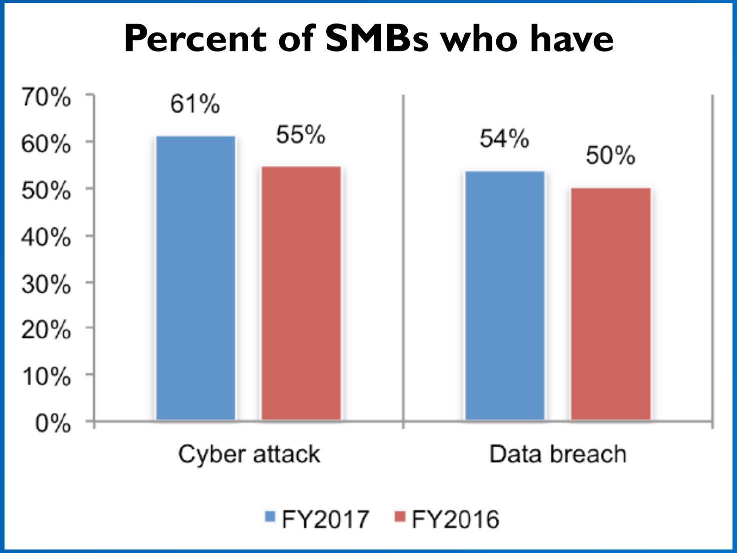
"Failing to Plan is Planning to Fail!"

PELL CENTER *for* INTERNATIONAL RELATIONS *and* PUBLIC POLICY

#PBNCYBER SUMMIT

SMALL & MEDIUM-SIZED BUSINESSES ARE A PRIME TARGET

- **52% of SMBs** experienced a ransomware attack in the past year, up from 2% the previous year.
- 58% of malware attack victims are small businesses;
- Over 66% of small business would go under if they suffered a cyber attack.



2017 State of Cybersecurity in Small & Medium Sized Business (SMB)
Ponemon Institute, Sept 2017

The number one cause of cyber breaches are a company's own employees!

PELL CENTER *for* INTERNATIONAL RELATIONS *and* PUBLIC POLICY

#PBNCYBER SUMMIT

RISKSENSE OVERVIEW

Company

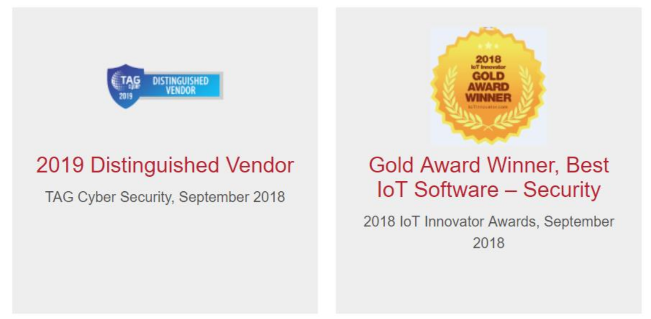
- Founded in 2015, Sunnyvale, CA and Albuquerque, NM
- CACTUS (US Congress): Computational Analysis of Cyber Terrorism against the US
- NSA/DHS National Academic Centers of Excellence
- Early Warning of WannaCry and Developed First RFID Fragmented Malware

Solutions

- Vulnerability and Threat Prioritization
- Attack surface validation and verification
- Attack monitoring and early warning of Threats
- Continuous and relative risk scoring

INTELLIGENT CYBER RISK PLATFORM

RiskSense is disrupting the cyber risk market with a Risk-as-a-Service based platform.

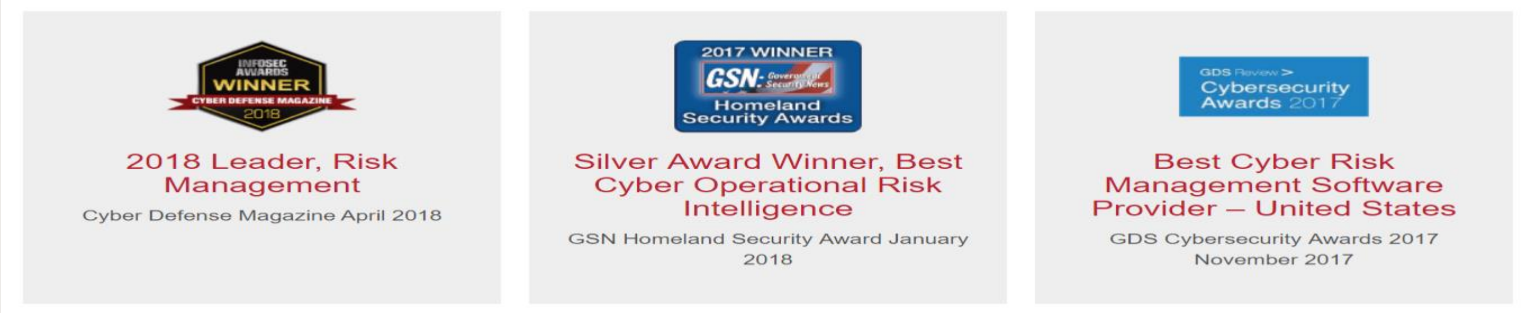

TAG DISTINGUISHED VENDOR 2019
2018 IoT Innovator GOLD AWARD WINNER

2019 Distinguished Vendor

TAG Cyber Security, September 2018

Gold Award Winner, Best IoT Software – Security

2018 IoT Innovator Awards, September 2018


INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2018
2017 WINNER GSN Government Security News Homeland Security Awards
GDS Review > Cybersecurity Awards 2017

2018 Leader, Risk Management

Cyber Defense Magazine April 2018

Silver Award Winner, Best Cyber Operational Risk Intelligence

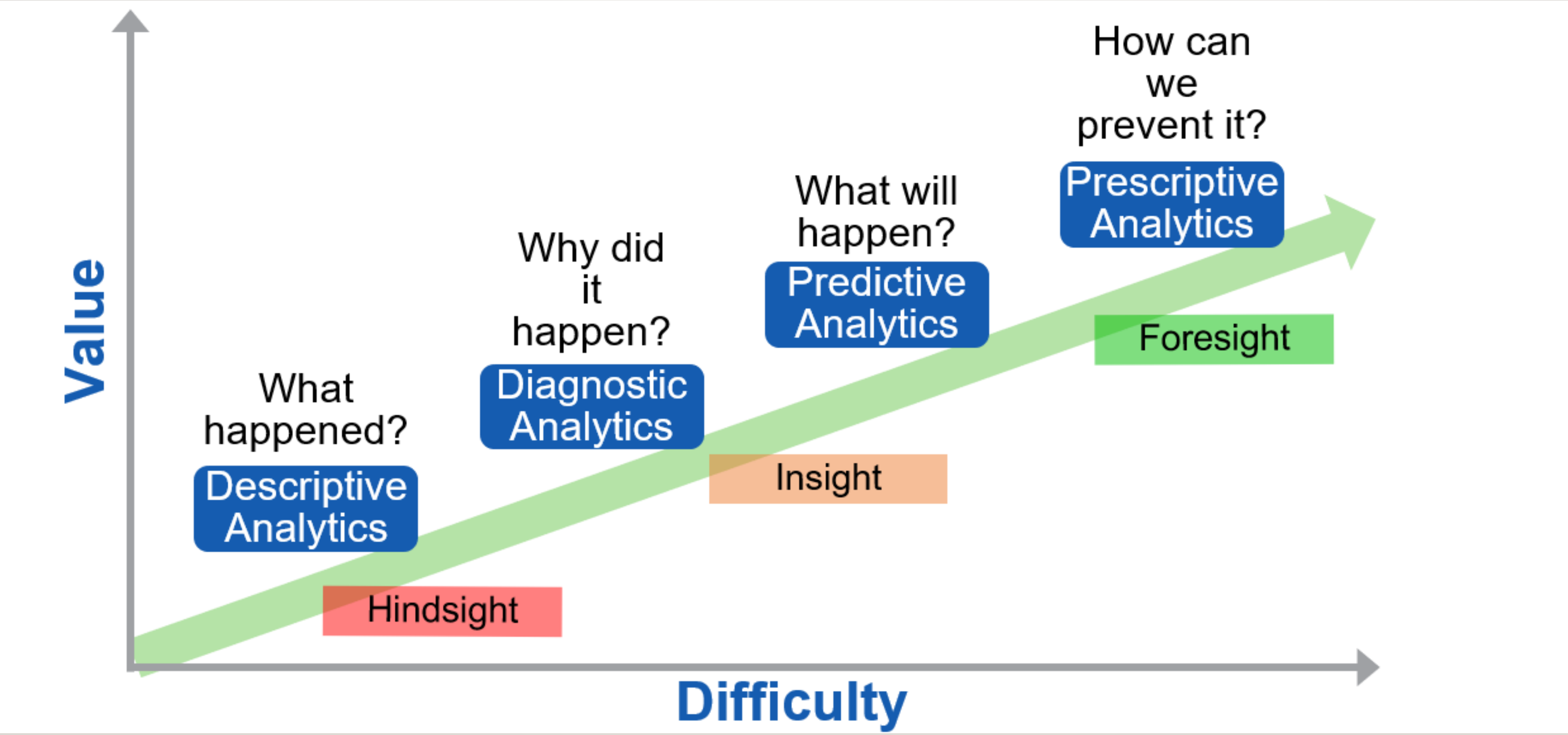
GSN Homeland Security Award January 2018

Best Cyber Risk Management Software Provider – United States

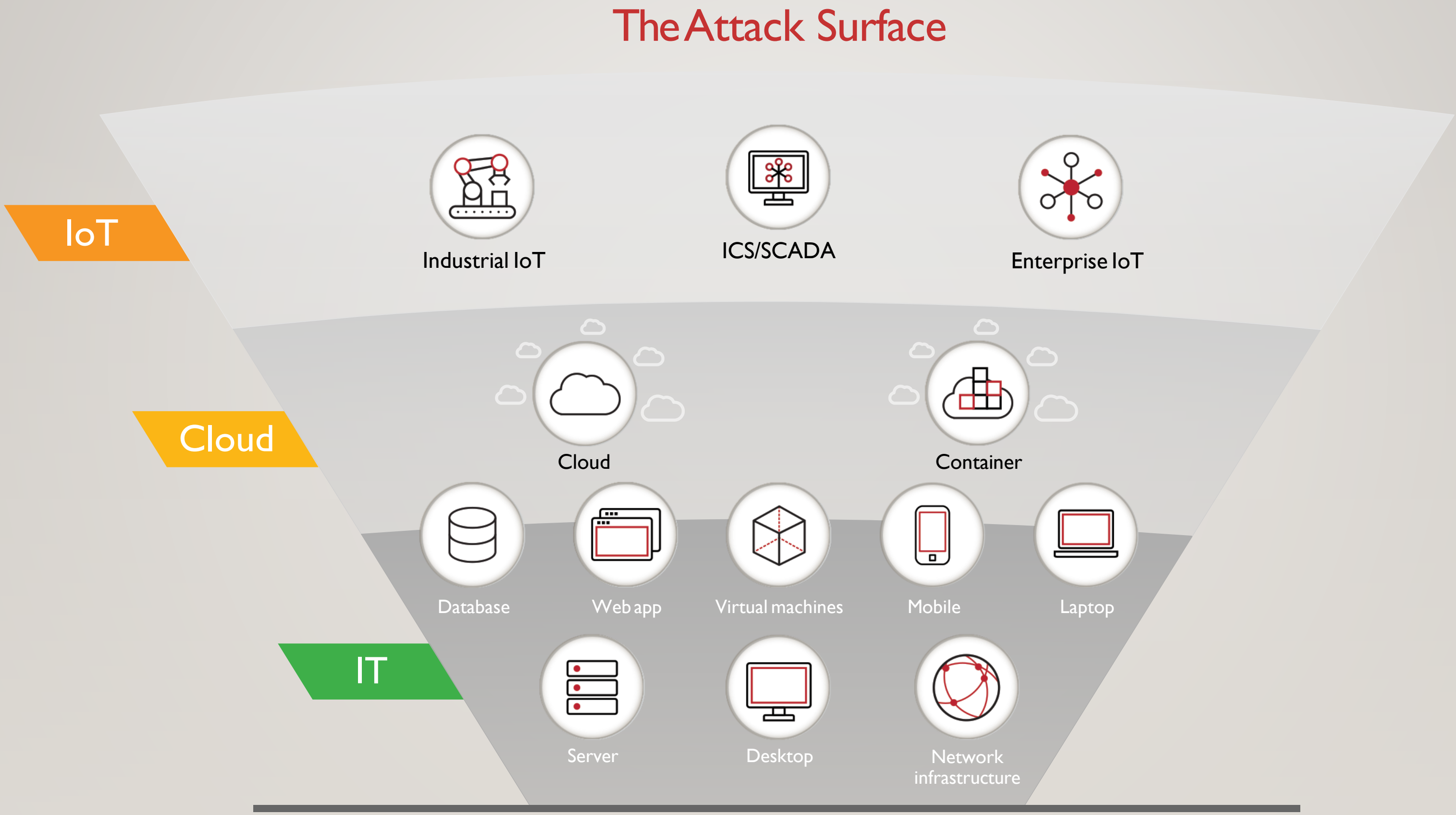
GDS Cybersecurity Awards 2017 November 2017

https://www.risksense.com/company/about-risksense/

Proactive & Preventative



DIGITAL TRANSFORMATION IS LEADING TO EXPONENTIAL GROWTH OF ATTACK SURFACE



NEW ERA OF SECURITY – CYBER RISK MANAGEMENT

Your Organization Will Be Hacked and Breached

Are you prepared?
How fast can you respond?

THE PROBLEM

Known Security Vulnerabilities are the Leading Cause of Data Breaches

100K

Vulnerabilities

Number of Unique Vulnerabilities (CVEs)

7X

Number of Assets

Average Number of Critical Vulnerabilities per Asset = 7

60+

Days

Average Time to Remediate a Critical Vulnerabilities

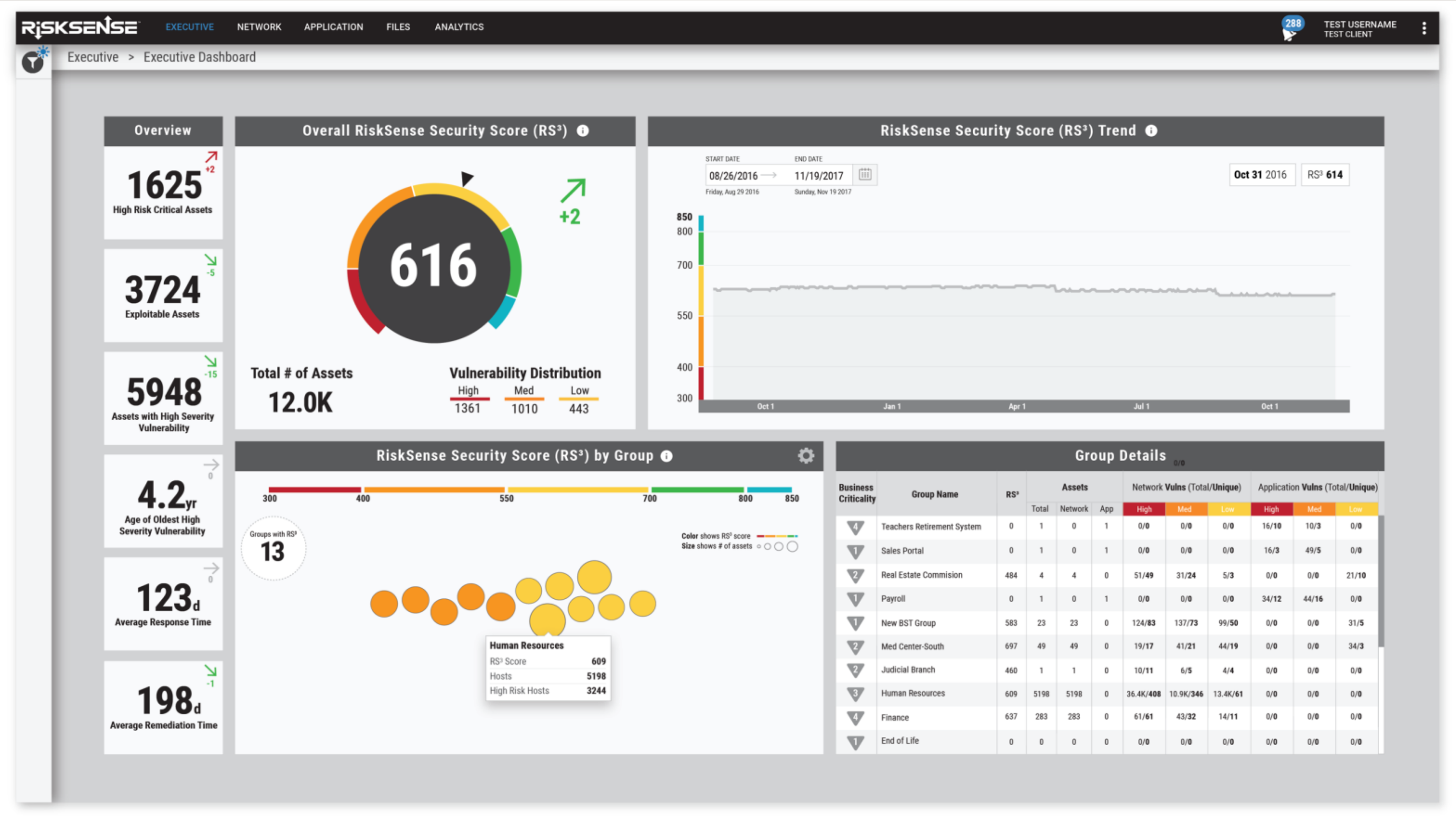
Most Security Tools Produce a Lot of Data without Context

No Visibility
& Hard to Collaborate

Hard to Measure & Manage Risk

Lack of Prioritization

EXECUTIVE DASHBOARD



Executive > Executive Dashboard

Overview

1625 (+2) High Risk Critical Assets

3724 (-5) Exploitable Assets

5948 (-15) Assets with High Severity Vulnerability

4.2yr (0) Age of Oldest High Severity Vulnerability

123d (0) Average Response Time

198d (-1) Average Remediation Time

Overall RiskSense Security Score (RS³)

616 +2

Total # of Assets 12.0K

Vulnerability Distribution

High	Med	Low
1361	1010	443

RiskSense Security Score (RS³) Trend

START DATE 08/26/2016 → END DATE 11/19/2017
Friday, Aug 29 2016 — Sunday, Nov 19 2017

Oct 31 2016 — RS³ 614

RiskSense Security Score (RS³) by Group

Groups with RS³ 13

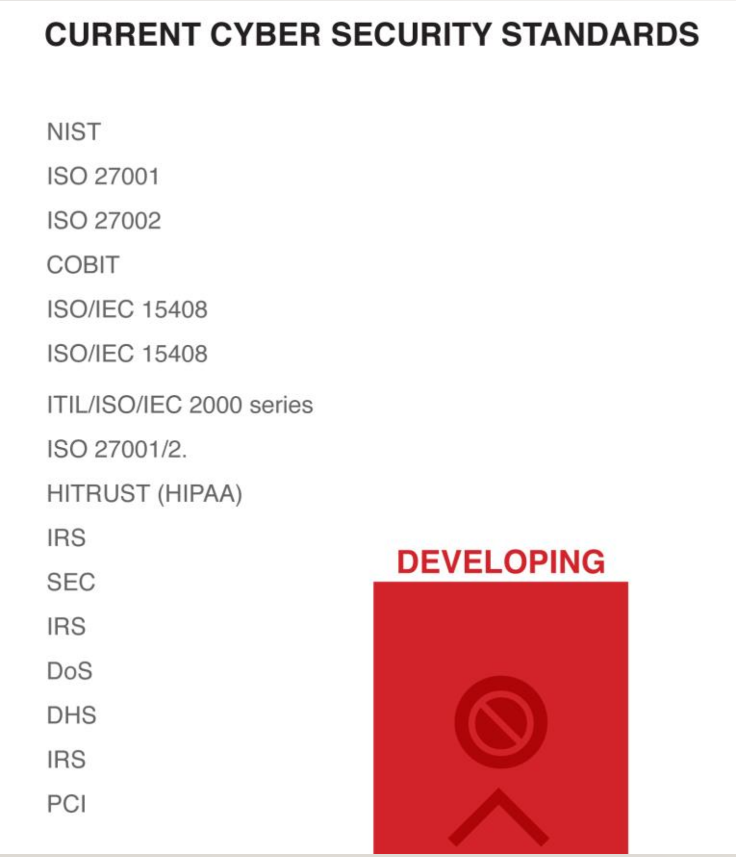
Human Resources

RS³ Score	609
Hosts	5198
High Risk Hosts	3244

Group Details

Business Criticality	Group Name	RS³	Assets			Network Vulns (Total/Unique)			Application Vulns (Total/Unique)		
			Total	Network	App	High	Med	Low	High	Med	Low
4	Teachers Retirement System	0	1	0	1	0/0	0/0	0/0	16/10	10/3	0/0
1	Sales Portal	0	1	0	1	0/0	0/0	0/0	16/3	49/5	0/0
2	Real Estate Commision	484	4	4	0	51/49	31/24	5/3	0/0	0/0	21/10
1	Payroll	0	1	0	1	0/0	0/0	0/0	34/12	44/16	0/0
1	New BST Group	583	23	23	0	124/83	137/73	99/50	0/0	0/0	31/5
2	Med Center-South	697	49	49	0	19/17	41/21	44/19	0/0	0/0	34/3
2	Judicial Branch	460	1	1	0	10/11	6/5	4/4	0/0	0/0	0/0
3	Human Resources	609	5198	5198	0	36.4K/408	10.9K/346	13.4K/61	0/0	0/0	0/0
4	Finance	637	283	283	0	61/61	43/32	14/11	0/0	0/0	0/0
1	End of Life	0	0	0	0	0/0	0/0	0/0	0/0	0/0	0/0

Cyber Security Journey



CURRENT CYBER SECURITY STANDARDS

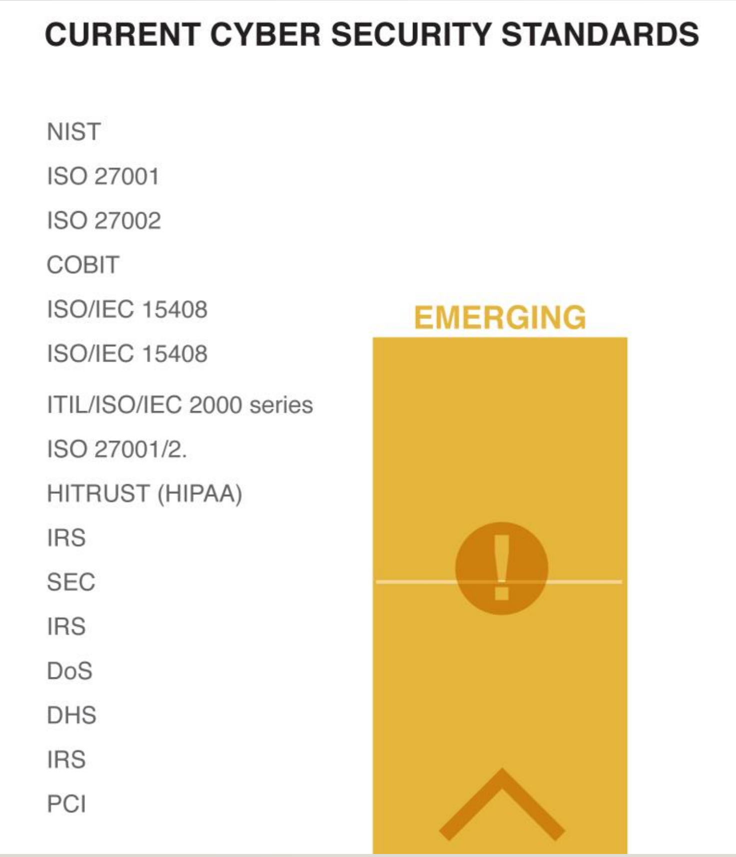
NIST
ISO 27001
ISO 27002
COBIT
ISO/IEC 15408
ISO/IEC 15408
ITIL/ISO/IEC 2000 series
ISO 27001/2.
HITRUST (HIPAA)
IRS
SEC
IRS
DoS
DHS
IRS
PCI

DEVELOPING

Compliance-Centric

- - Annual orientation
- - Activity based
- - Record keeping
- - Basic standards
- - Not contextual, continuous or threat-adaptive
- *“Checking the boxes”*

Cyber Security Journey



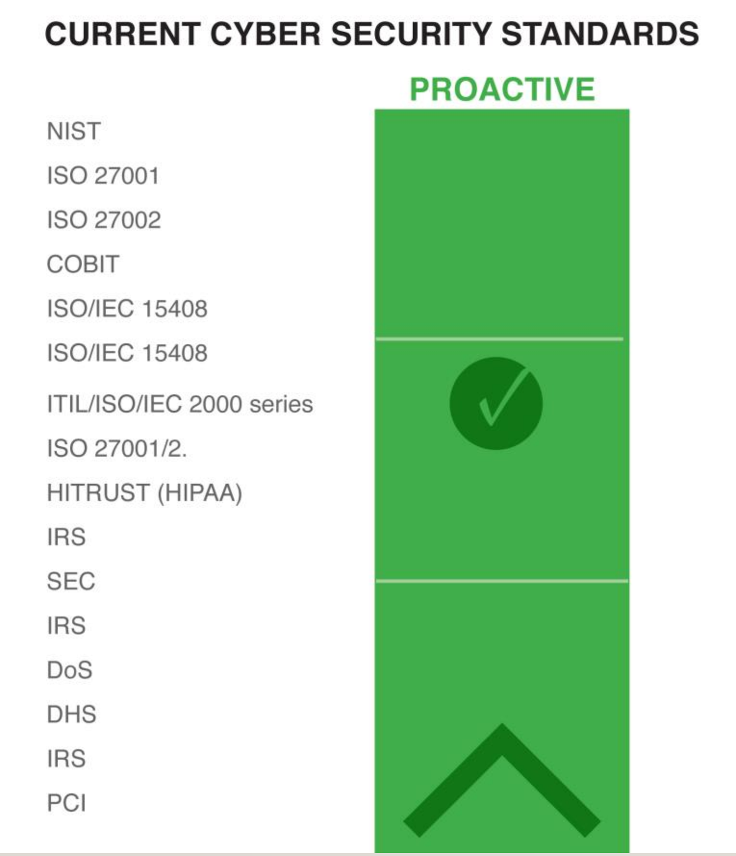
CURRENT CYBER SECURITY STANDARDS

NIST
ISO 27001
ISO 27002
COBIT
ISO/IEC 15408
ISO/IEC 15408
ITIL/ISO/IEC 2000 series
ISO 27001/2.
HITRUST (HIPAA)
IRS
SEC
IRS
DoS
DHS
IRS
PCI

Increasing Compliance

- - Semi-annual or quarterly
- - Role definition increasing
- - Processes maturing
- - Increased standard rigor
- - Not contextual, continuous or threat-adaptive
- *“Compliance emerging in importance”*

Cyber Security Journey



CURRENT CYBER SECURITY STANDARDS

PROACTIVE

NIST
ISO 27001
ISO 27002
COBIT
ISO/IEC 15408
ISO/IEC 15408
ITIL/ISO/IEC 2000 series
ISO 27001/2.
HITRUST (HIPAA)
IRS
SEC
IRS
DoS
DHS
IRS
PCI

Proactive & Preventative

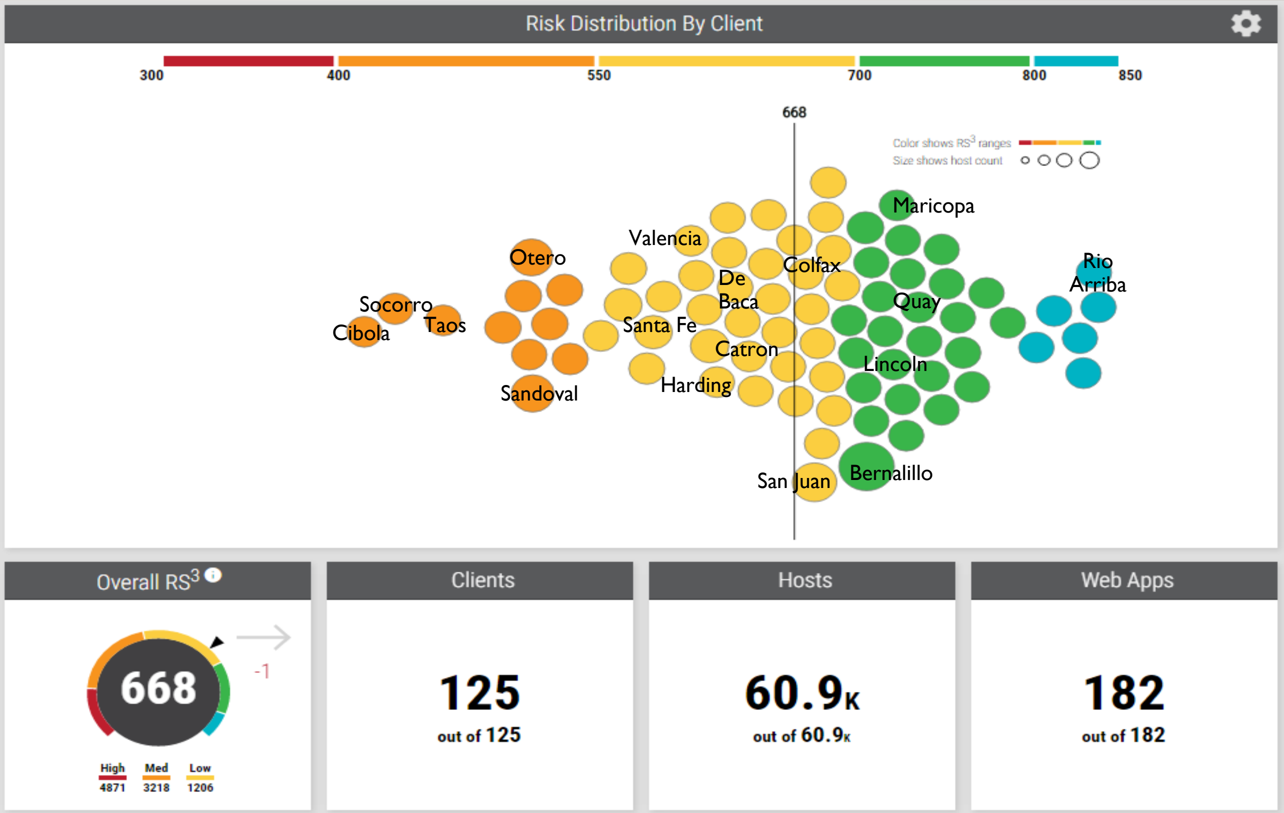
- - Cadence is continuous
- - Prioritization based on risk
- - Process maturity based on a unified focus
- - Visibility up and down the chain of command
- - Contextual, continuous and threat-adaptive
- *“Compliance is a byproduct”*

RISKSENSE – MULTI-CLIENT DASHBOARD

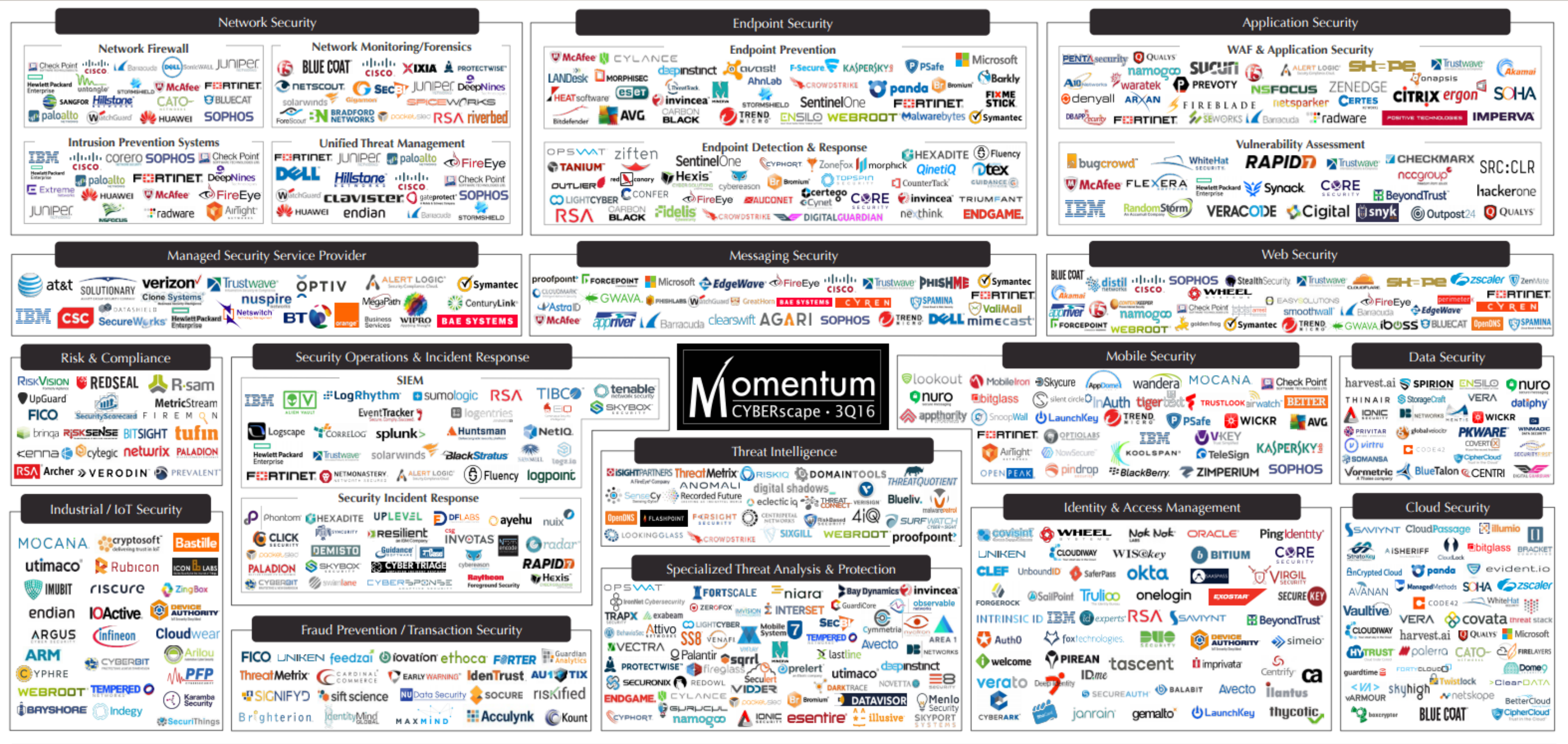
EXAMPLE: STATE OF NEW MEXICO WITH REPRESENTATIVE COUNTIES

Data for all Entities:

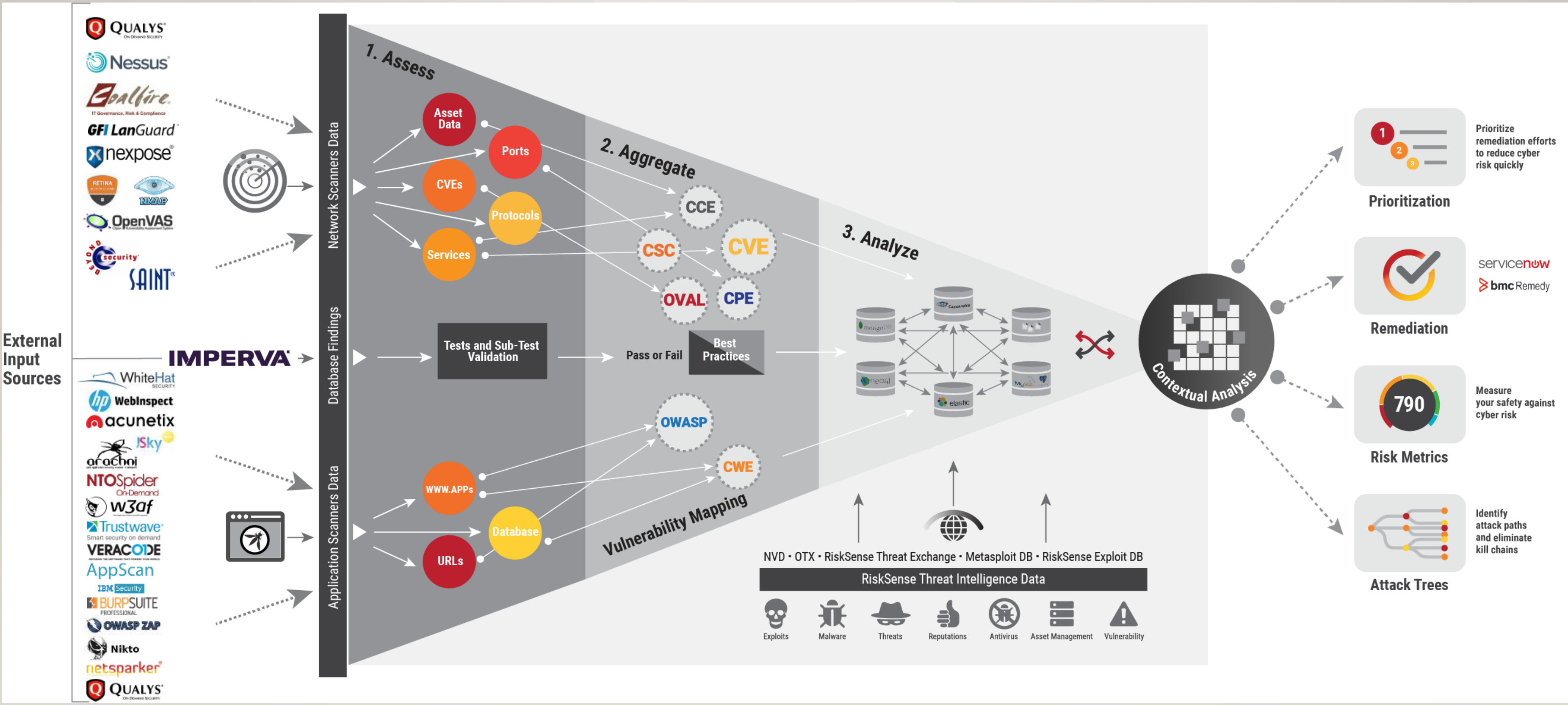
- RiskSense Distribution Map
    - Color-coded by RiskSense Security Score (RS3) Range
- Overall RS3 score
    - Vulnerability distribution
    - Daily trending info
- Total number of hosts
- Total number of web applications



IT-Centric Cyber Security – Which tool?


Network Security
Network Firewall
Network Monitoring/Forensics
Intrusion Prevention Systems
Unified Threat Management
Endpoint Security
Endpoint Prevention
Endpoint Detection & Response
Application Security
WAF & Application Security
Vulnerability Assessment
Managed Security Service Provider
Messaging Security
Web Security
Risk & Compliance
Security Operations & Incident Response
SIEM
Security Incident Response
Momentum CYBERscape · 3Q16
Mobile Security
Data Security
Threat Intelligence
Industrial / IoT Security
Fraud Prevention / Transaction Security
Specialized Threat Analysis & Protection
Identity & Access Management
Cloud Security

RISKSENSE PLATFORM (SAAS)



THE COST OF CYBER BREACH

"Cyber-attacks are the number one problem facing mankind, even worse than nuclear weapons."

- Warren Buffett

- A new global study conducted by IBM suggests the ***financial impact of a data breach for an organization is, on average, $3.86 million***.
- In the ***worst cases, "mega breaches" may cost the enterprise between $40 million and $350 million***.
- The average time it took to uncover a data breach is ***197 days***, and once identified, it takes roughly ***69 days*** to contain.
- However, the ***speed of incident response teams can have a huge impact*** on the overall cost of a data breach.
- When a breach is contained in less than a month, IBM suggests businesses may be able to ***save up to $1 million*** in comparison to slower companies.

PANEL 2

Colin Coleman
Partner
Partridge Snow & Hahn

Cindy Lepore
Client Executive/
Business Insurance
Marsh McLennan Agency

Larry Selnick
Director, Treasury &
Payment Solutions
Webster Bank

Eric Shorr
President
Secure Future
Tech Solutions

PROVIDENCE BUSINESS NEWS PBN SUMMIT CYBERSECURITY

Colin Coleman

Partner

PARTRIDGE
SNOW &
HAHN LLP

#PBNCYBER SUMMIT

Cindy Lepore

Client Executive/ Business Insurance

MARSH & McLENNAN AGENCY

#PBNCYBER SUMMIT

Larry Selnick

Director, Treasury & Payment Solutions

WebsterBank

#PBNCYBER SUMMIT

PROVIDENCE BUSINESS NEWS
PBN SUMMIT
CYBERSECURITY

Eric Shorr

President

SecureFuture
TECH SOLUTIONS
Proactive Today for a Brighter Tomorrow

#PBNCYBER SUMMIT

PANEL 2

Colin Coleman
Partner
Partridge Snow & Hahn

Cindy Lepore
Client Executive/
Business Insurance
Marsh McLennan Agency

Larry Selnick
Director, Treasury &
Payment Solutions
Webster Bank

Eric Shorr
President
Secure Future
Tech Solutions

#PBNCYBER SUMMIT

MARSH & McLENNAN AGENCY

2018 PBN CYBER SUMMIT

October 11, 2018 | Crowne Plaza

Cindy Lepore
Client Executive | Business Insurance

Marsh & McLennan Agency
MMA-NE.com

WORLD CLASS. LOCAL TOUCH.

2018 PBN Cyber Summit
Agenda

I. About The Panelist

II. Cyber Liability Insurance

III. Summary

2018 PBN CYBER SUMMIT

ABOUT THE PANELIST

ABOUT THE PANELIST
CINDY LEPORE, CLCS AND GSC CYBERSECURITY AND INTELLIGENCE

Cindy Lepore
Client Executive, Property & Casualty
Marsh & McLennan Agency

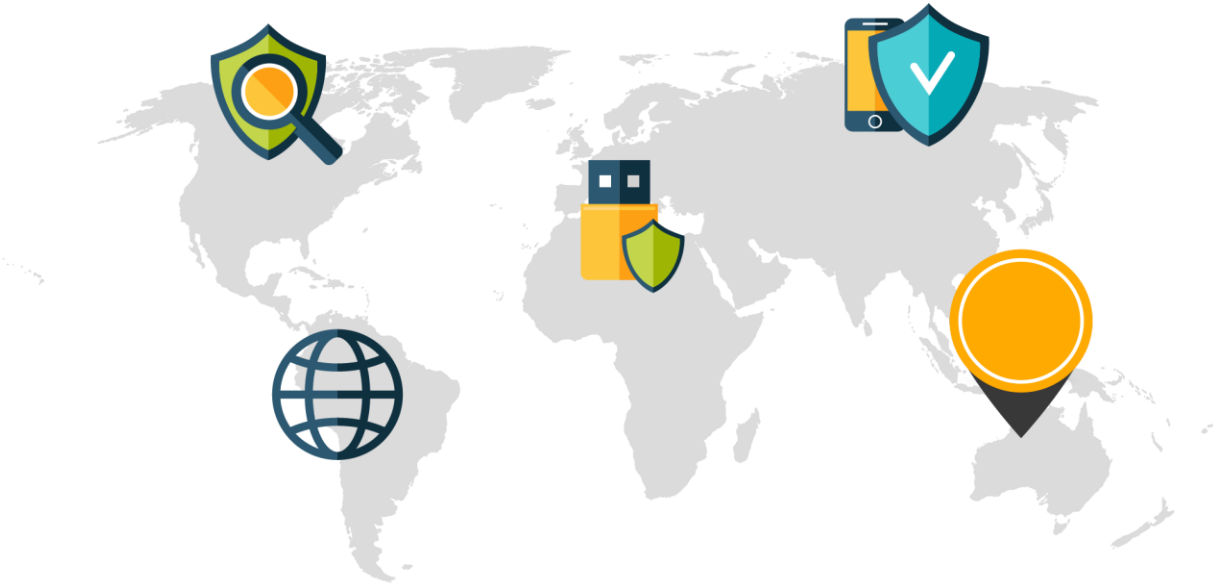
- Business Insurance-Cybersecurity Champion New England
- Over 20 years in Telecom and IT
- Disciplines include Technology, Education, Non-Profit, Private and Advanced Manufacturing
- Member of the Rhode Island State Police Cyber Task Force and InfraGard
- Graduate of Bryant University
- MBA program Salve Regina University

2018 PBN CYBER SUMMIT

POTENTIAL COSTS & LOSSES

2018 PBN Cyber Summit
Potential Costs and Losses

- Brand Deterioration
- Legal Liability
- Regulatory
- Data Assets
- First Party
- Third Party
- Business Interruption



2018 PBN CYBER SUMMIT

CRISIS MANAGEMENT

2018 PBN Cyber Summit
Crisis Management

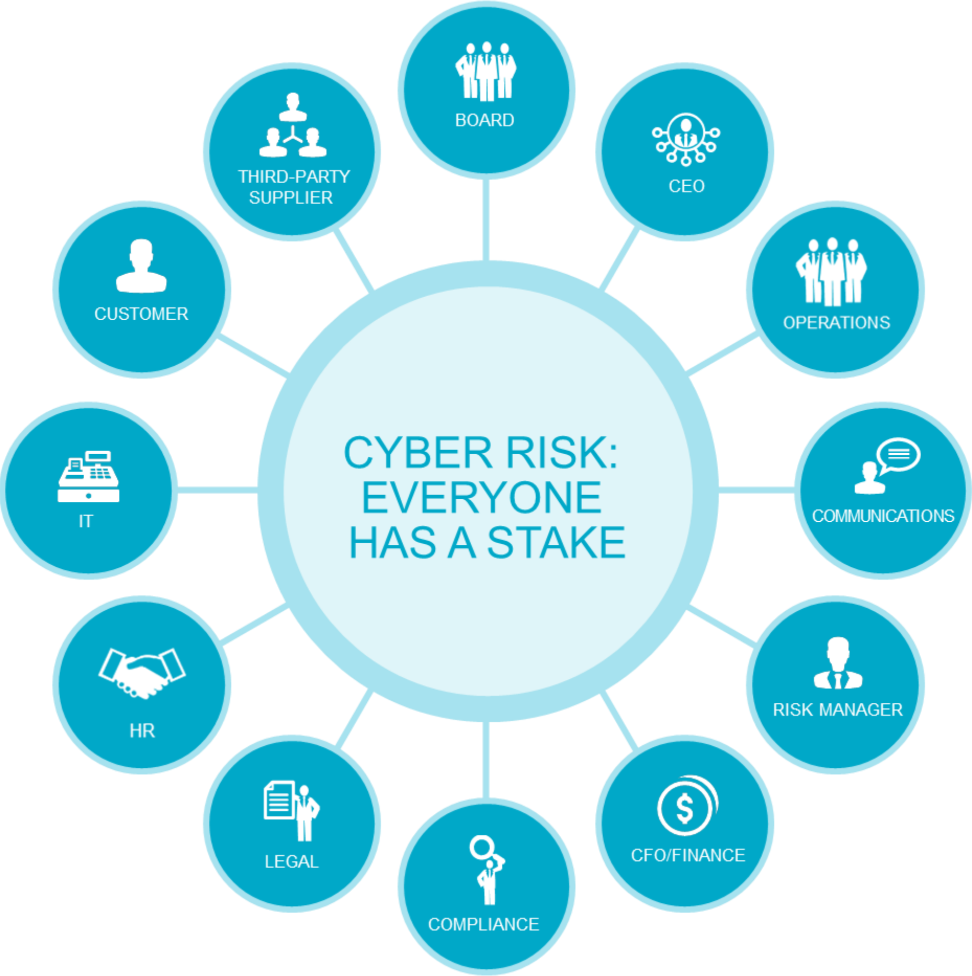
- Legal Costs
- Notification Cost
- Computer Forensic Costs
- Credit Monitoring and Identity Theft Protection Costs
- Public Relations and Crisis Management Consultancy Costs

2018 PBN CYBER SUMMIT
STAKEHOLDERS

CYBER RISK – EVERYONE HAS A STAKE

"Cost of data breach will reach 2.1 trillion globally by 2019."

-JUNIPER



2018 PBN CYBER SUMMIT

SUMMARY

Summary

- Transfer Risk
- Plan Your Cyber Strategy
- Train and Educate All Employees
- Use a broker who is experienced

MARSH & McLENNAN
AGENCY

Cindy Lepore
Client Executive, Business Insurance
Marsh & McLennan Agency
Cindy.Lepore@marshmma.com

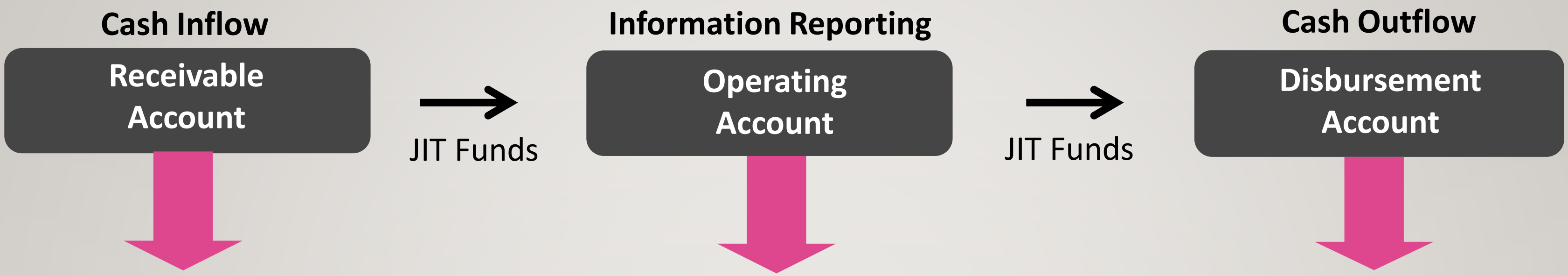
MMA New England is a part of Marsh & McLennan Agency, LLC (MMA). Securities offered through MMA Securities LLC (MMA Securities), member FINRA / SIPC, and a federally registered investment advisor. Main Office: 1166 Avenue of the Americas, New York, NY 10036. Phone: (212) 345-5000. Variable insurance products distributed by MMA Securities LLC. MMA and MMA Securities are affiliates owned by Marsh & McLennan Companies.

This document is not intended to be taken as advice regarding any individual situation and should not be relied upon as such. Marsh & McLennan Agency LLC shall have no obligation to update this publication and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting or legal matters are based solely on our experience as consultants and are not to be relied upon as actuarial, accounting, tax or legal advice, for which you should consult your own professional advisors. Any modeling analytics or projections are subject to inherent uncertainty and the analysis could be materially affective if any underlying assumptions, conditions, information or factors are inaccurate or incomplete or should change.

How to Mitigate Risk

Banking Security in Layers

Recommend dedicated accounts for receivable, operating, and disbursement accounts :



Cash Inflow

Receivable Account

JIT Funds

Information Reporting

Operating Account

JIT Funds

Cash Outflow

Disbursement Account

- Post no debits
- No ACH or wire origination capability
- Mandatory Alerts

- (2x) Daily Cash Position
- Just in Time (JIT) Transfers
- Mandatory Alerts

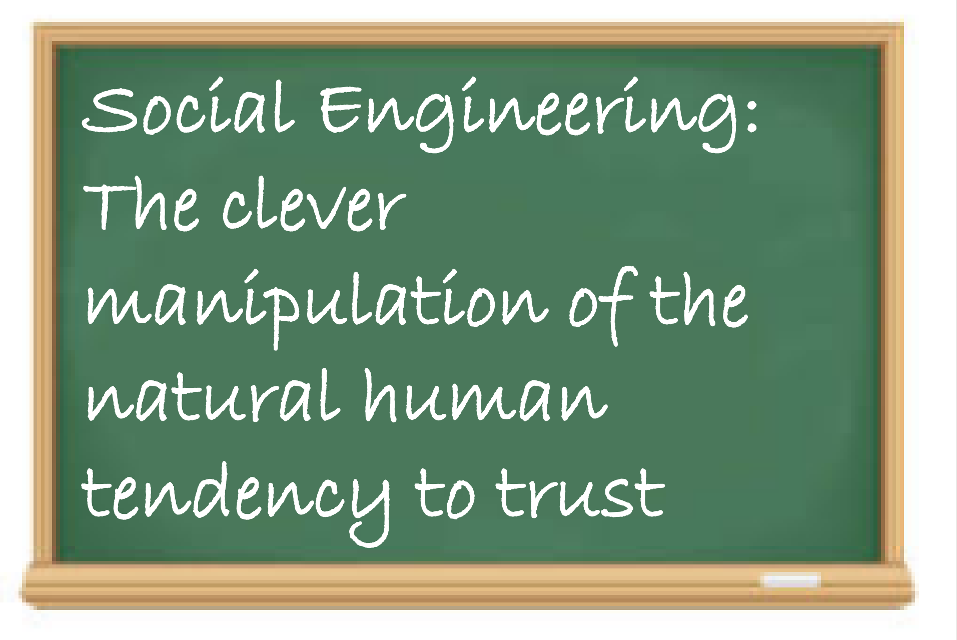
- **Check Positive Pay**
- **ACH Positive Pay**
- Controlled Disbursement
- Daily Review/ reconciliations
- Mandatory Alerts
- **Dual Control/Tiered security (separate and distinct access)**
- Limits set to business needs

- Separate Account for check and EFT activities
- Dedicated PC (Separate Independent Workstations – segregated networks)
- Up-to-Date Anti-Virus, Anti-Malware, and Up-to-Date other Network Controls recommended by IT Support
- Ongoing and Regular Employee, Vendor and Partner Education, and security awareness training

Types of Fraud

E-Mail Account Compromise

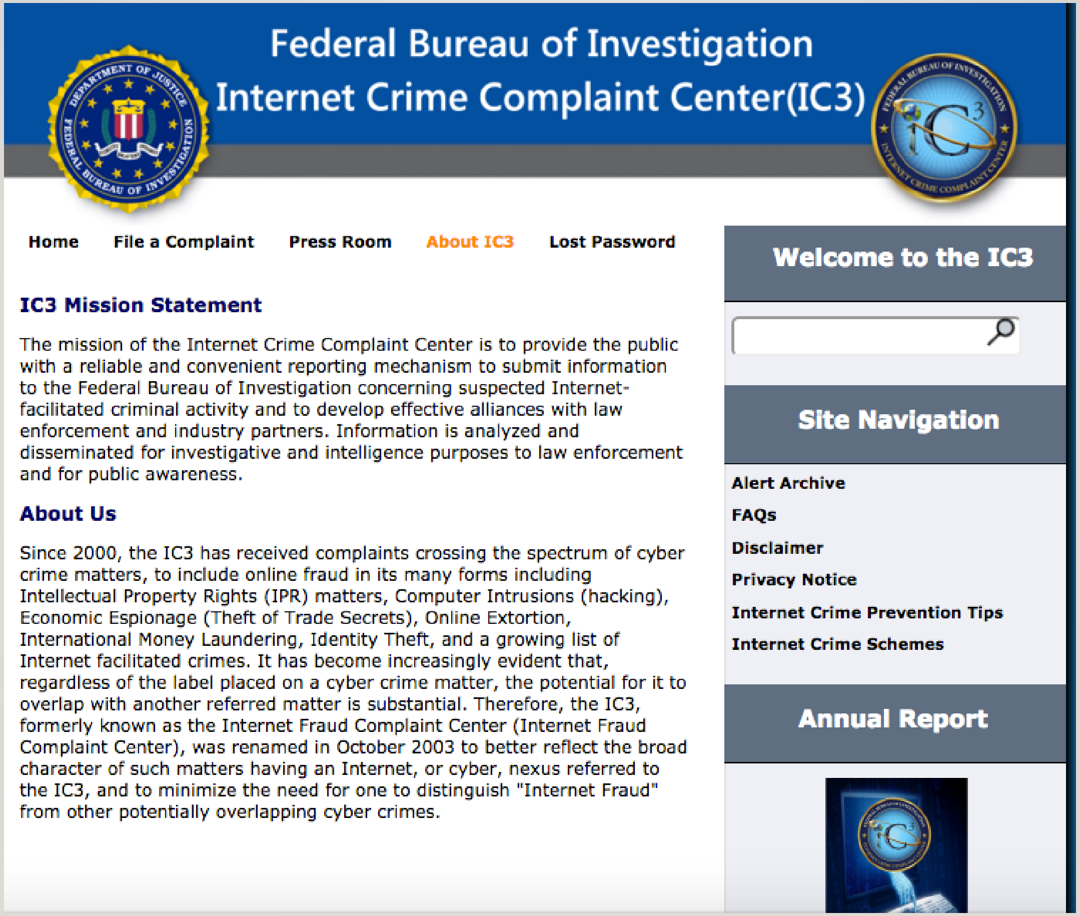
- **E-mail Account Compromise (EAC) is a sophisticated scam that targets the general public and professionals associated with, but not limited to, financial and lending institutions, real estate companies, and law firms.**
- **The EAC scam is very similar to the Business E-mail Compromise (BEC) scam, except that it targets individuals rather than businesses.**
- **2017, IC3 received a total of 301,580 complaints with reported losses in excess of $1.4 billion!**



Social Engineering:
The clever manipulation of the natural human tendency to trust

TYPES OF FRAUD

FBI Internet Crime Complaint (www.ic3.gov)



IC3 Mission Statement

The mission of the Internet Crime Complaint Center is to provide the public with a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation concerning suspected Internet-facilitated criminal activity and to develop effective alliances with law enforcement and industry partners. Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness.

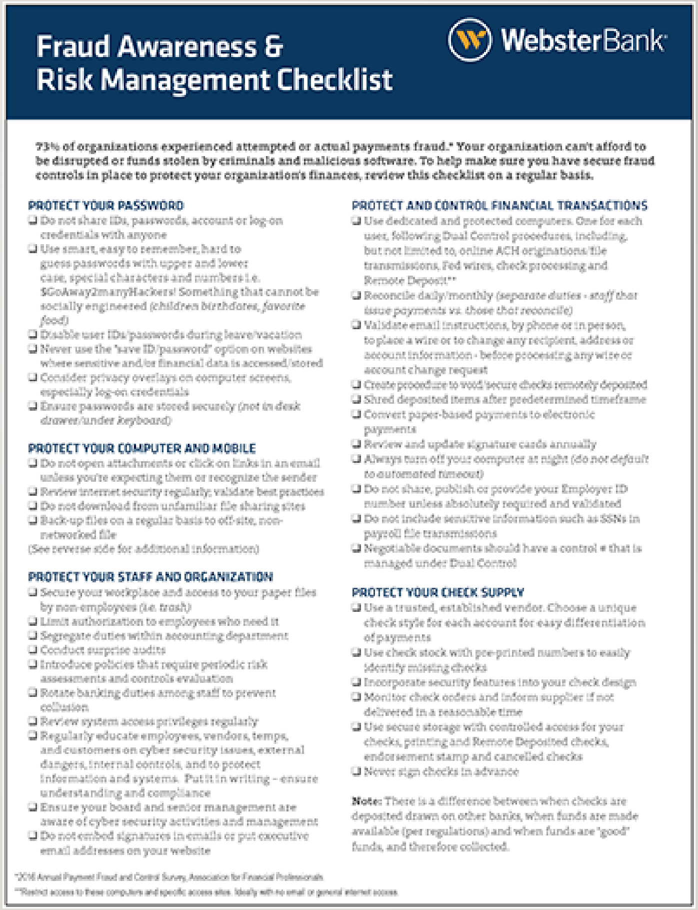
About Us

Since 2000, the IC3 has received complaints crossing the spectrum of cyber crime matters, to include online fraud in its many forms including Intellectual Property Rights (IPR) matters, Computer Intrusions (hacking), Economic Espionage (Theft of Trade Secrets), Online Extortion, International Money Laundering, Identity Theft, and a growing list of Internet facilitated crimes. It has become increasingly evident that, regardless of the label placed on a cyber crime matter, the potential for it to overlap with another referred matter is substantial. Therefore, the IC3, formerly known as the Internet Fraud Complaint Center (Internet Fraud Complaint Center), was renamed in October 2003 to better reflect the broad character of such matters having an Internet, or cyber, nexus referred to the IC3, and to minimize the need for one to distinguish "Internet Fraud" from other potentially overlapping cyber crimes.

HOW TO MITIGATE RISK

Fraud Checklist

- Engage your Partners:
    - Accountant
    - Insurance
        - Cyber Liability
    - Legal
        - Involve your Practice Partners
    - IT Consultant
        - Forensic IT on call
    - Banker
    - Public Relations



Fraud Awareness & Risk Management Checklist

WebsterBank

73% of organizations experienced attempted or actual payments fraud.* Your organization can't afford to be disrupted or funds stolen by criminals and malicious software. To help make sure you have secure fraud controls in place to protect your organization's finances, review this checklist on a regular basis.

PROTECT YOUR PASSWORD

- ❑ Do not share IDs, passwords, account or log-on credentials with anyone
- ❑ Use smart, easy to remember, hard to guess passwords with upper and lower case, special characters and numbers i.e. $GoAway2manyHackers! Something that cannot be socially engineered *(children birthdates, favorite food)*
- ❑ Disable user IDs/passwords during leave/vacation
- ❑ Never use the "save ID/password" option on websites where sensitive and/or financial data is accessed/stored
- ❑ Consider privacy overlays on computer screens, especially log-on credentials
- ❑ Ensure passwords are stored securely *(not in desk drawer/under keyboard)*

PROTECT YOUR COMPUTER AND MOBILE

- ❑ Do not open attachments or click on links in an email unless you're expecting them or recognize the sender
- ❑ Review internet security regularly; validate best practices
- ❑ Do not download from unfamiliar file sharing sites
- ❑ Back-up files on a regular basis to off-site, non-networked file

(See reverse side for additional information)

PROTECT YOUR STAFF AND ORGANIZATION

- ❑ Secure your workplace and access to your paper files by non-employees *(i.e. trash)*
- ❑ Limit authorization to employees who need it
- ❑ Segregate duties within accounting department
- ❑ Conduct surprise audits
- ❑ Introduce policies that require periodic risk assessments and controls evaluation
- ❑ Rotate banking duties among staff to prevent collusion
- ❑ Review system access privileges regularly
- ❑ Regularly educate employees, vendors, temps, and customers on cyber security issues, external dangers, internal controls, and to protect information and systems. Put it in writing – ensure understanding and compliance
- ❑ Ensure your board and senior management are aware of cyber security activities and management
- ❑ Do not embed signatures in emails or put executive email addresses on your website

PROTECT AND CONTROL FINANCIAL TRANSACTIONS

- ❑ Use dedicated and protected computers. One for each user, following Dual Control procedures, including, but not limited to, online ACH originations/file transmissions, Fed wires, check processing and Remote Deposit**
- ❑ Reconcile daily/monthly *(separate duties - staff that issue payments vs. those that reconcile)*
- ❑ Validate email instructions, by phone or in person, to place a wire or to change any recipient, address or account information - before processing any wire or account change request
- ❑ Create procedure to void/secure checks remotely deposited
- ❑ Shred deposited items after predetermined timeframe
- ❑ Convert paper-based payments to electronic payments
- ❑ Review and update signature cards annually
- ❑ Always turn off your computer at night *(do not default to automated timeout)*
- ❑ Do not share, publish or provide your Employer ID number unless absolutely required and validated
- ❑ Do not include sensitive information such as SSNs in payroll file transmissions
- ❑ Negotiable documents should have a control # that is managed under Dual Control

PROTECT YOUR CHECK SUPPLY

- ❑ Use a trusted, established vendor. Choose a unique check style for each account for easy differentiation of payments
- ❑ Use check stock with pre-printed numbers to easily identify missing checks
- ❑ Incorporate security features into your check design
- ❑ Monitor check orders and inform supplier if not delivered in a reasonable time
- ❑ Use secure storage with controlled access for your checks, printing and Remote Deposited checks, endorsement stamp and cancelled checks
- ❑ Never sign checks in advance

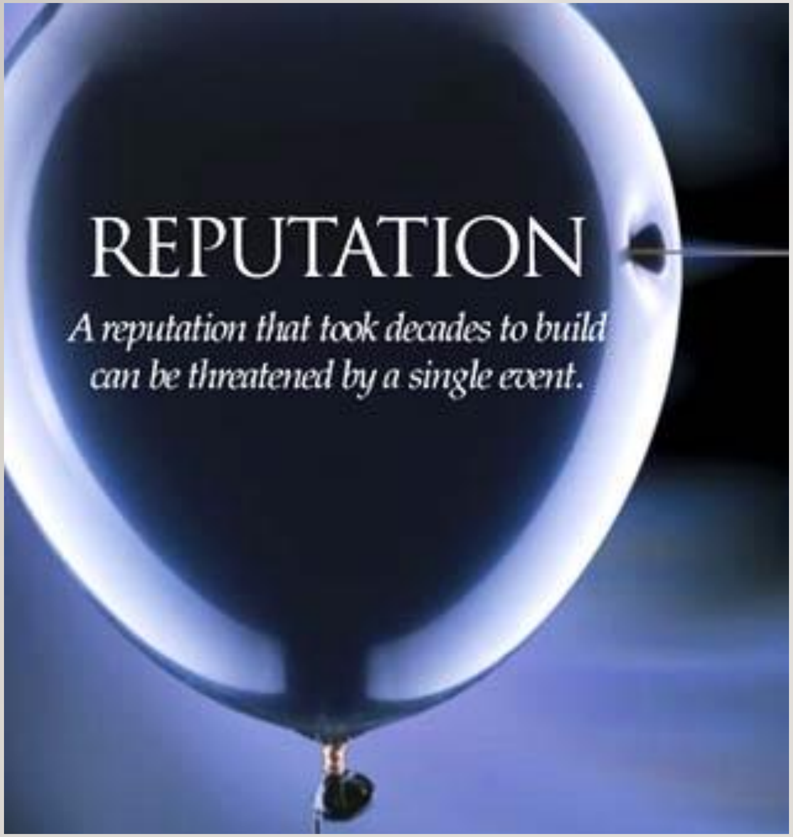
Note: There is a difference between when checks are deposited drawn on other banks, when funds are made available (per regulations) and when funds are "good" funds, and therefore collected.

*2016 Annual Payment Fraud and Control Survey, Association for Financial Professionals

**Restrict access to these computers and specific access sites. Ideally with no email or general internet access.

Value of Your Reputation…

Priceless!


REPUTATION
A reputation that took decades to build
can be threatened by a single event.

- The true costs to business from threats are far greater than merely the financial implications.
- In addition to direct costs there are:
  - The cost of computer downtime
  - Plummeting productivity
  - Lost sales opportunities
  - Regulatory fines
  - Worried Customers
  - Concerned vendors

PANEL 2

Colin Coleman
Partner
Partridge Snow & Hahn

Cindy Lepore
Client Executive/
Business Insurance
Marsh McLennan Agency

Larry Selnick
Director, Treasury &
Payment Solutions
Webster Bank

Eric Shorr
President
Secure Future
Tech Solutions

#PBNCYBER SUMMIT

PROVIDENCE BUSINESS NEWS

PBN SUMMIT

CYBERSECURITY

October 11, 2018

#PBNCYBER SUMMIT

PROVIDENCE BUSINESS NEWS
PBN
SUMMIT
CYBERSECURITY

thank you…

PRESENTING SPONSOR

BlumShapiro

Accounting | Tax | Business Consulting

#PBNCYBER SUMMIT

PROVIDENCE BUSINESS NEWS
PBN SUMMIT
CYBERSECURITY

thank you…

PRESENTING SPONSOR

PARTRIDGE
SNOW &
HAHN LLP

#PBNCYBER SUMMIT

PROVIDENCE BUSINESS NEWS
PBN SUMMIT
CYBERSECURITY

thank you…

PARTNER SPONSOR

BRYANT UNIVERSITY 1863

Bryant University

Executive Development Center

#PBNCYBER SUMMIT

PROVIDENCE BUSINESS NEWS
PBN
SUMMIT
CYBERSECURITY

thank you…

PARTNER SPONSOR

COX
Business®

#PBNCYBER SUMMIT

PROVIDENCE BUSINESS NEWS
PBN
SUMMIT
CYBERSECURITY

thank you…

PARTNER SPONSOR

MARSH & McLENNAN
AGENCY

PROVIDENCE BUSINESS NEWS
PBN SUMMIT
CYBERSECURITY

thank you…

PARTNER SPONSOR

SecureFuture
TECH SOLUTIONS
Proactive Today for a Brighter Tomorrow

#PBNCYBER SUMMIT

PROVIDENCE BUSINESS NEWS
PBN
SUMMIT
CYBERSECURITY

thank you…

PARTNER SPONSOR

WebsterBank

#PBNCYBER SUMMIT

PROVIDENCE BUSINESS NEWS

PBN SUMMIT CYBERSECURITY

October 11, 2018

#PBNCYBER SUMMIT