HIMSS VIRGINIA Chapter

NOVEMBER 5~7, 2018

WILLIAMSBURG, VA

#VAHIMSS18

Topical Talk
Third Party Risk

Richard Staynings @rstaynings

SVP, Chief Security & Trust Officer, Clearwater

HIMSS Privacy & Security Committee

Board Member AEHIS

What’s the connection between this man and the Second Largest Retailer in the United States?

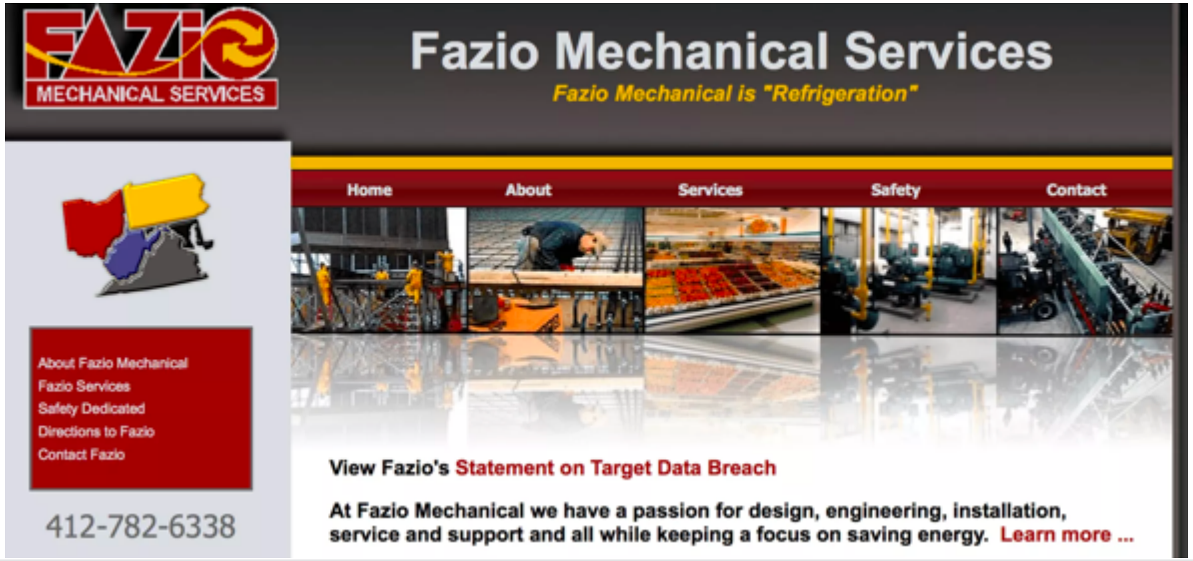
His company cost the retailer Hundreds of Millions of Dollars … and resulted in the firing of its Entire Executive Leadership Team

Fazio Mechanical Services - Sharpsburg, PA

Ross E. Fazio
President

Ross A. Fazio
Executive Vice President

Jeff Rupert
VP Operations



Fazio Mechanical Services

Fazio Mechanical is "Refrigeration"

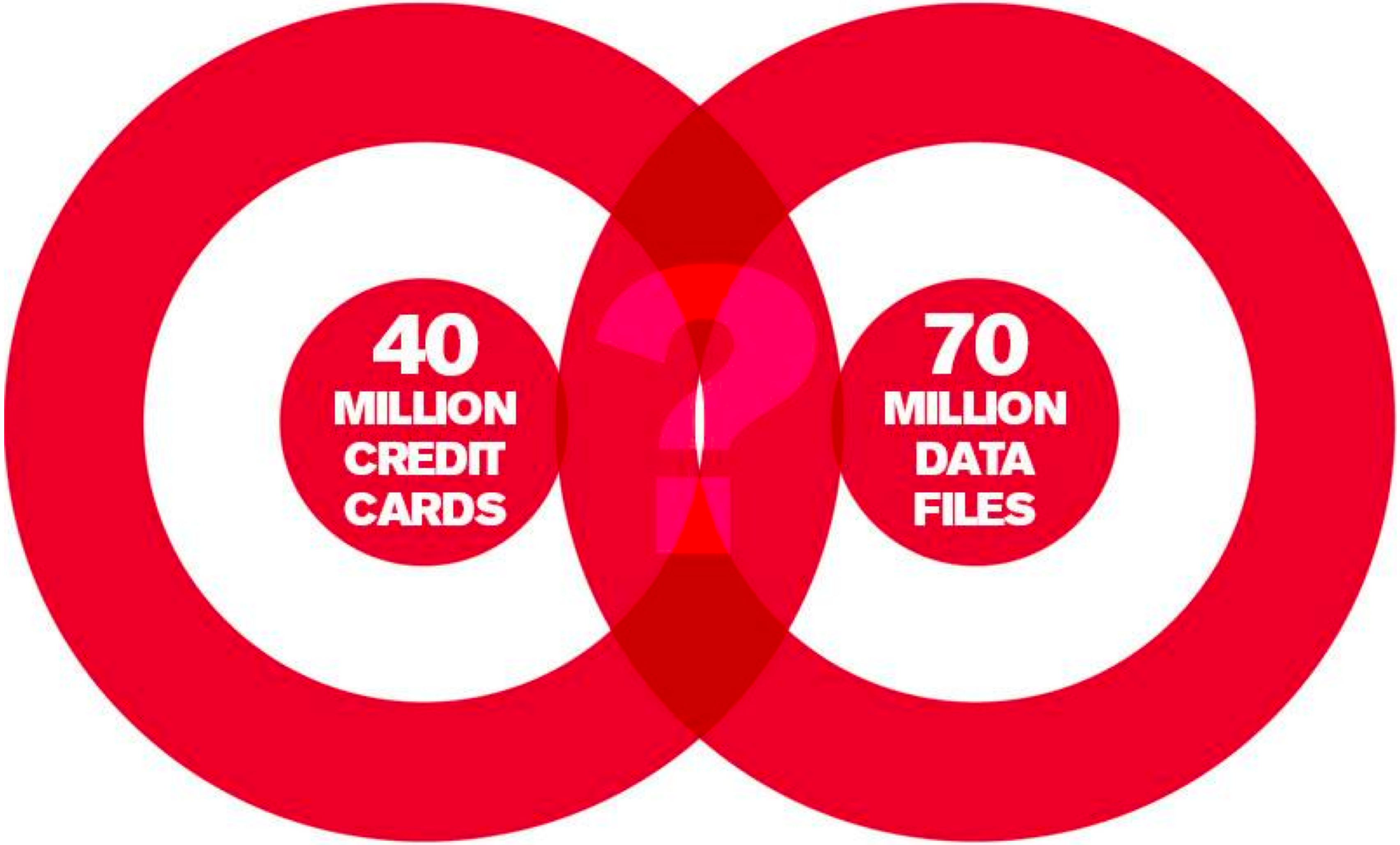
412-782-6338

View Fazio's Statement on Target Data Breach

At Fazio Mechanical we have a passion for design, engineering, installation, service and support and all while keeping a focus on saving energy. Learn more ...

TARGET
HACKED

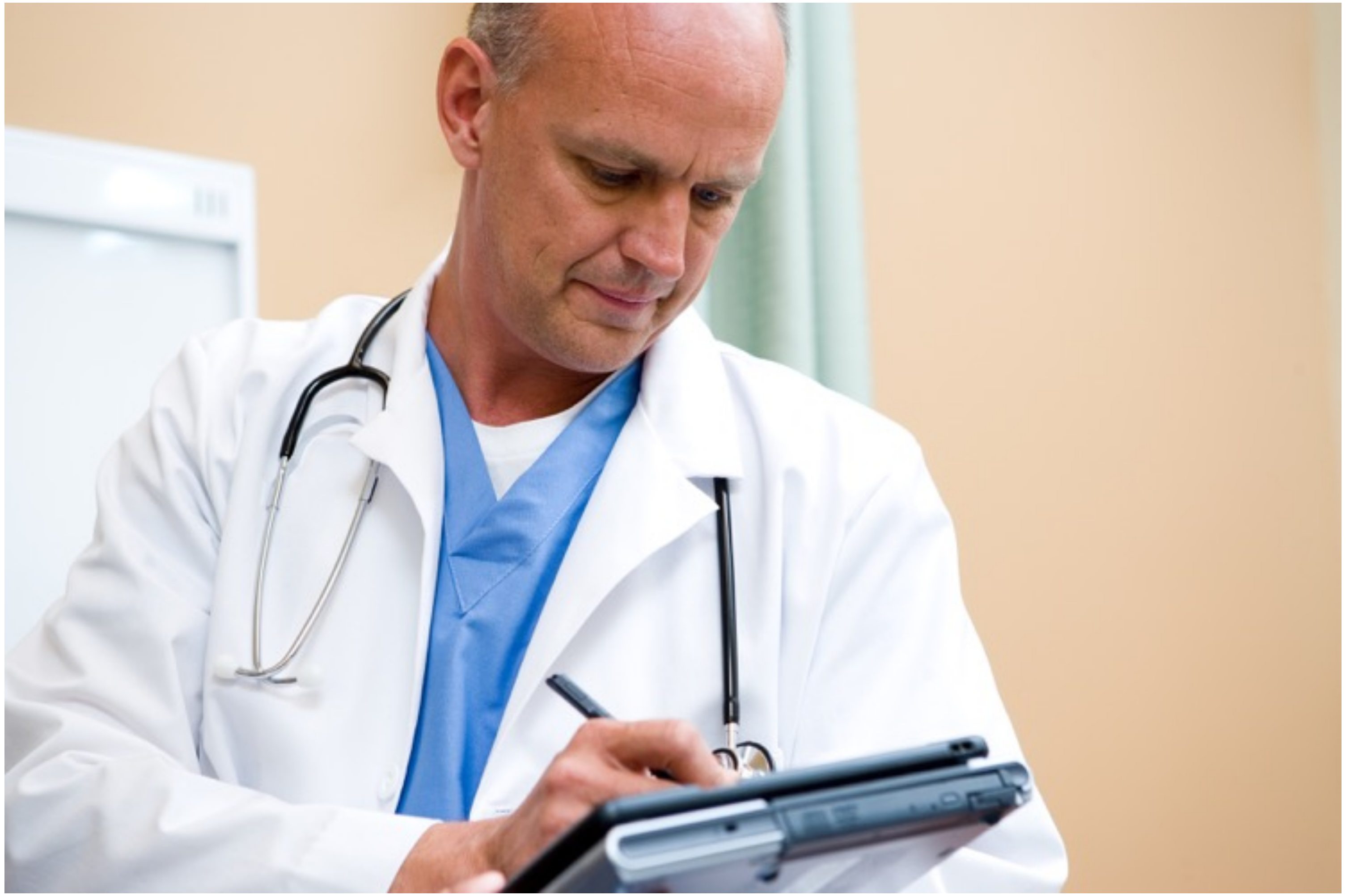
Target Stores Data Breach 2013



The Lesson

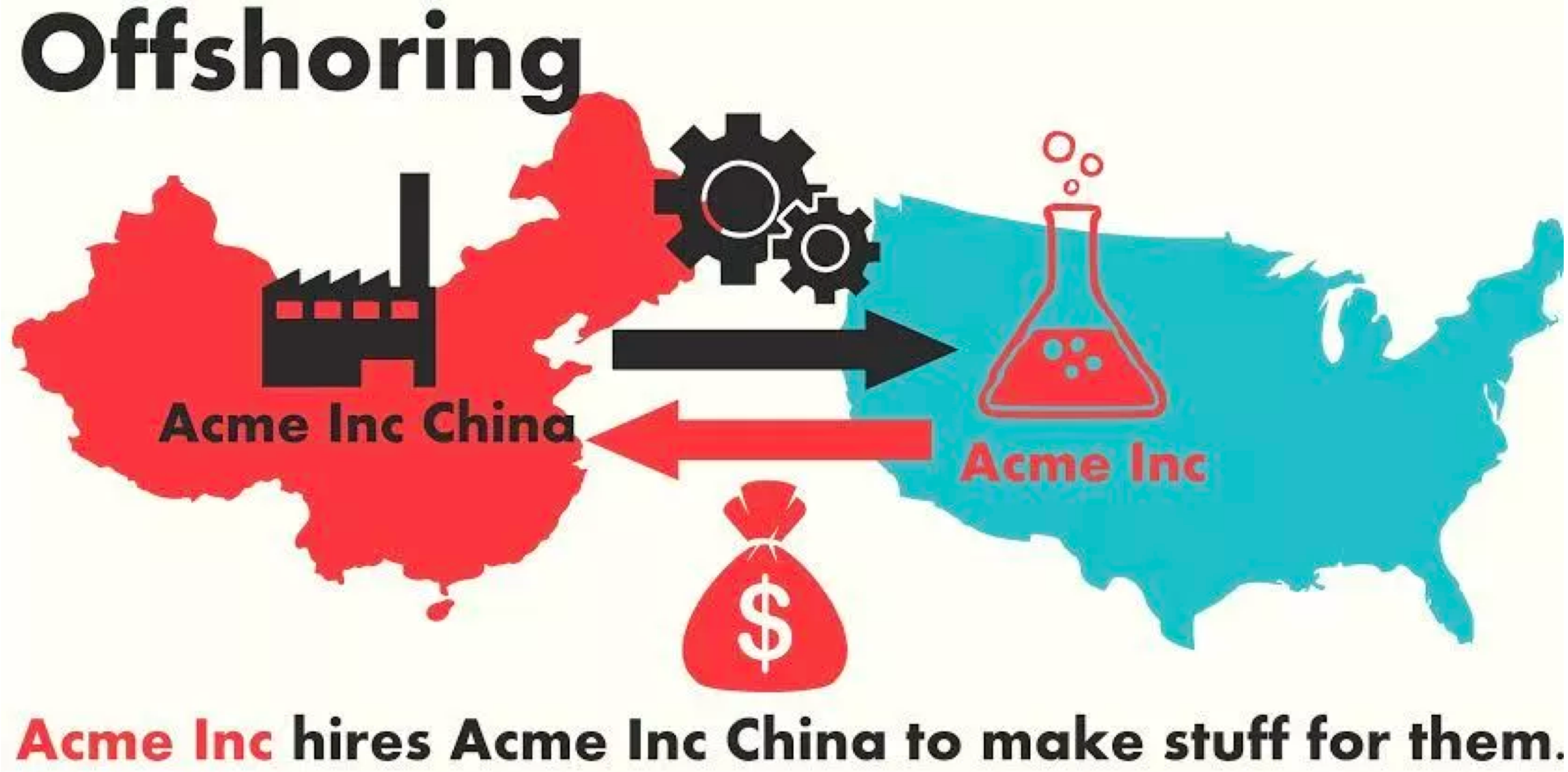
- It really does matter who your Vendors, Suppliers, Outsources and Service Providers are…..
- Especially if you provide them access to your network
- Especially of you provide them physical access to your promises
- AND …
- You want to keep your job!

Why is this important to Healthcare?



Unpresented level of BP and IT Outsourcing

Off-Shoring and Global Supply Lines



Off-Shoring

- Less then 10% of the iPhone is made in the USA.
- iPhone 7 series alone added $15.7 billion to the U.S. trade deficit with China last year
- Other manufacturers are worse!

Global Supply Chains

Whether you purchase iPhones or X-RAY machines, the manufacture and supply of these devices is complex and usually global

Industry Challenges

US Healthcare today is highly dependent upon an extensive global chain of:

Vendors
Suppliers
Partners
Outsourcers & Delivery Partners
Researchers
… and other third-parties

Nomenclature

For the sake of argument we’ll just call them all

‘VENDORS’

Nomenclature

… and the Process

‘TPVRM’

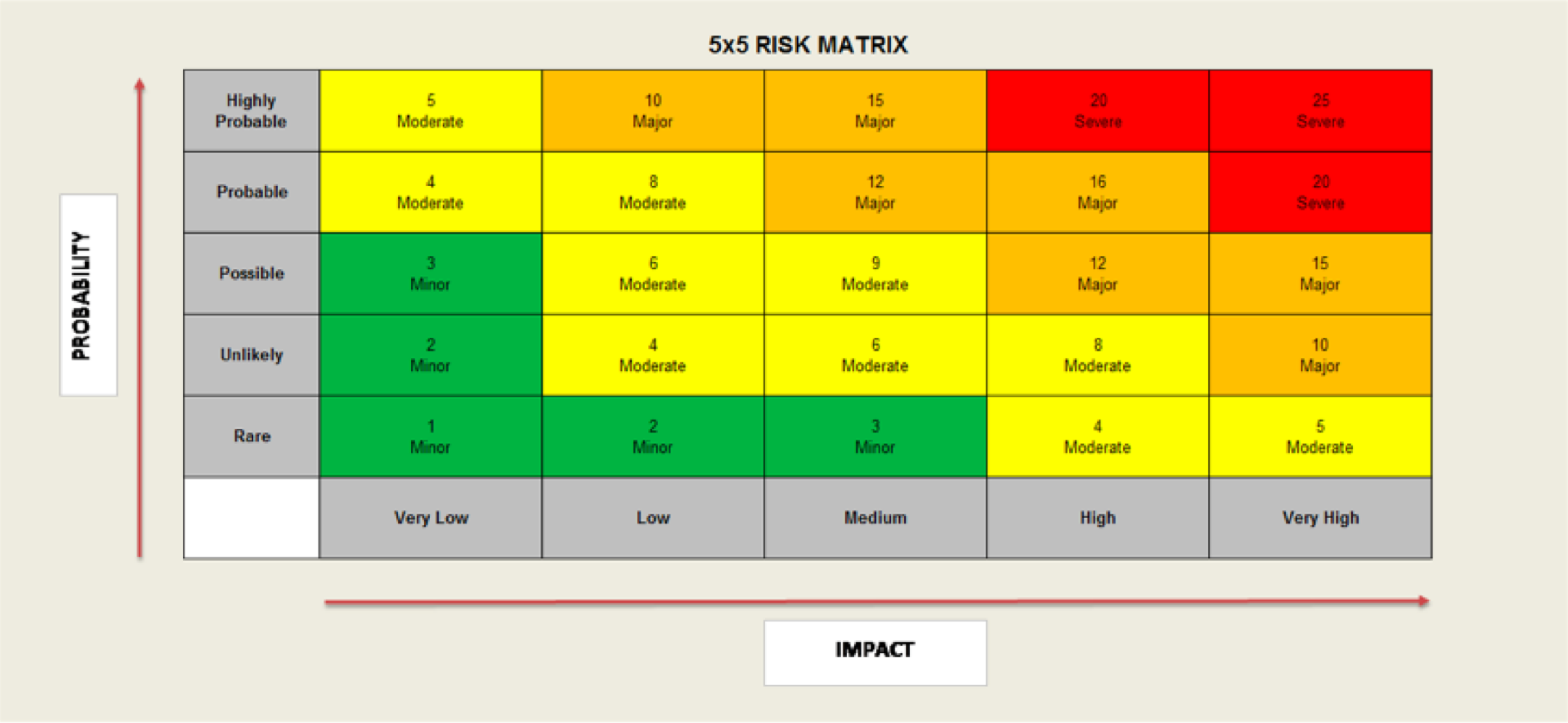
Trump Trade War

Threatens to introduce risk and cost into
the Global Supply Chain

Why is that important to my hospital?

- Because your vendors have vendors .. And your vendors have their own vendors too!
  - So ….Fourth Party Vendor Management
  - And….Fifth Party Vendor Management
  - Etc.
- Supply chains are long, complex and global in nature today
- Any interruption in the global supply chain will impact your hospital
- **AVAILABILITY** presents a **RISK**
- Remember that HIPAA requires you to secure the of **Confidentiality**, **Integrity** and **Availability** of Protected Health Information

How many of you perform a regular and ongoing Risk Analysis of each of your vendors?



5x5 RISK MATRIX

PROBABILITY

Highly Probable	5 Moderate	10 Major	15 Major	20 Severe	25 Severe
Probable	4 Moderate	8 Moderate	12 Major	16 Major	20 Severe
Possible	3 Minor	6 Moderate	9 Moderate	12 Major	15 Major
Unlikely	2 Minor	4 Moderate	6 Moderate	8 Moderate	10 Major
Rare	1 Minor	2 Minor	3 Minor	4 Moderate	5 Moderate
	Very Low	Low	Medium	High	Very High

IMPACT

HIMSS VIRGINIA Chapter

How many of you even have an up to date and complete list of all of your vendors?

If Not, then YOU SHOULD!

If Not, then YOU SHOULD!

By TOMORROW ideally

Third-Party Risk

A recent Vendor Vulnerability Index research report released by Bomgar, showed that breaches occurring from third parties account for **two-thirds of the total number of reported breaches**. *

* Bomgar. Vendor Vulnerability Index brings security risk of third-parties to light, April 2016

Third-Party Risk

The study also found that:

- Only **46%** of US companies said they know the number of log-ins that could be attributed to vendors

Third-Party Risk

The study also found that:

- Less than **51%** enforce policies around third party access

Third-Party Risk

The study also found that:

- 69% said they definitely or possibly suffered a security breach resulting from vendor access in the past year

Third-Party Risk

The consensus by Security Professionals is that the risk posed by third parties is not only **substantial**, but it is **increasing**.

Board Level Issue

Gartner stated in their June 2017 Magic Quadrant for IT Vendor Risk Management that by 2020, 75% of Fortune Global 500 companies will treat vendor risk management as a **board-level initiative to mitigate brand and reputation risk. ***

* Gartner. Magic Quadrant for IT Vendor Risk Management, June 2017

Gartner - Factors to Consider:

- Whether the vendor has custody of, or access to, your sensitive information (PHI, PII, IP)
- Whether the vendor has access to your company's network or physical access to your sites
- Size of the vendor
- Location of the vendor
- Sophistication of the vendor's IT and security teams
- Whether the vendor itself outsources services to **fourth parties**
- The vendor's product or service
- **Regulations**

HIMSS VIRGINIA *Chapter*

* Gartner. Magic Quadrant for IT Vendor Risk Management, June 2017

Here Are Some Questions You Should Ask Yourself

How do you manage Third-Party Risk?

- Do you know how many vendors you have?
- Do you categorize them?
- Does everyone who has access to your PHI sign a BAA - including research, pharma and medical device providers?
- Do you have standardized contract language across vendors?
- Who can sign an agreement or contract with a vendor?
- Are contracts and agreements reviewed by security and risk before acceptance?
- Do your contracts and BAAs provide a provision for you to regularly assess risks in conjunction with the services each vendor provides? How often do you ever exercise that right?
- How many people would it take for you to risk-assess all of your vendors annually?

How to you conduct Third Party Risk Analysis?

- Voluntary vendor risk questionnaire? – What percentage come back complete?
- Do you ever perform any validation?
- Do your vendor assessments or questionnaires meet the **NIST sp800-30** standard required by OCR for Risk Analysis?
- Do any vendors provide you with ISO 27001 certifications or SSAE18-SOC2-Type II attestations (or their equivalent)?
- Do you validate the control objectives in line with your risk objectives?
- How often to perform vendor assessments?

Let’s not kid ourselves, this is a HUGE Problem for most Covered Entities

What do we need to do to fix the TPVRM problem?

- Vendor categorization
- Proper Risk Assessments of Vendors that meets OCR guidelines and NIST standards (SP800-30)
- Risk Assessment Process Automation
- Sharing of Vendor Risk Ratings

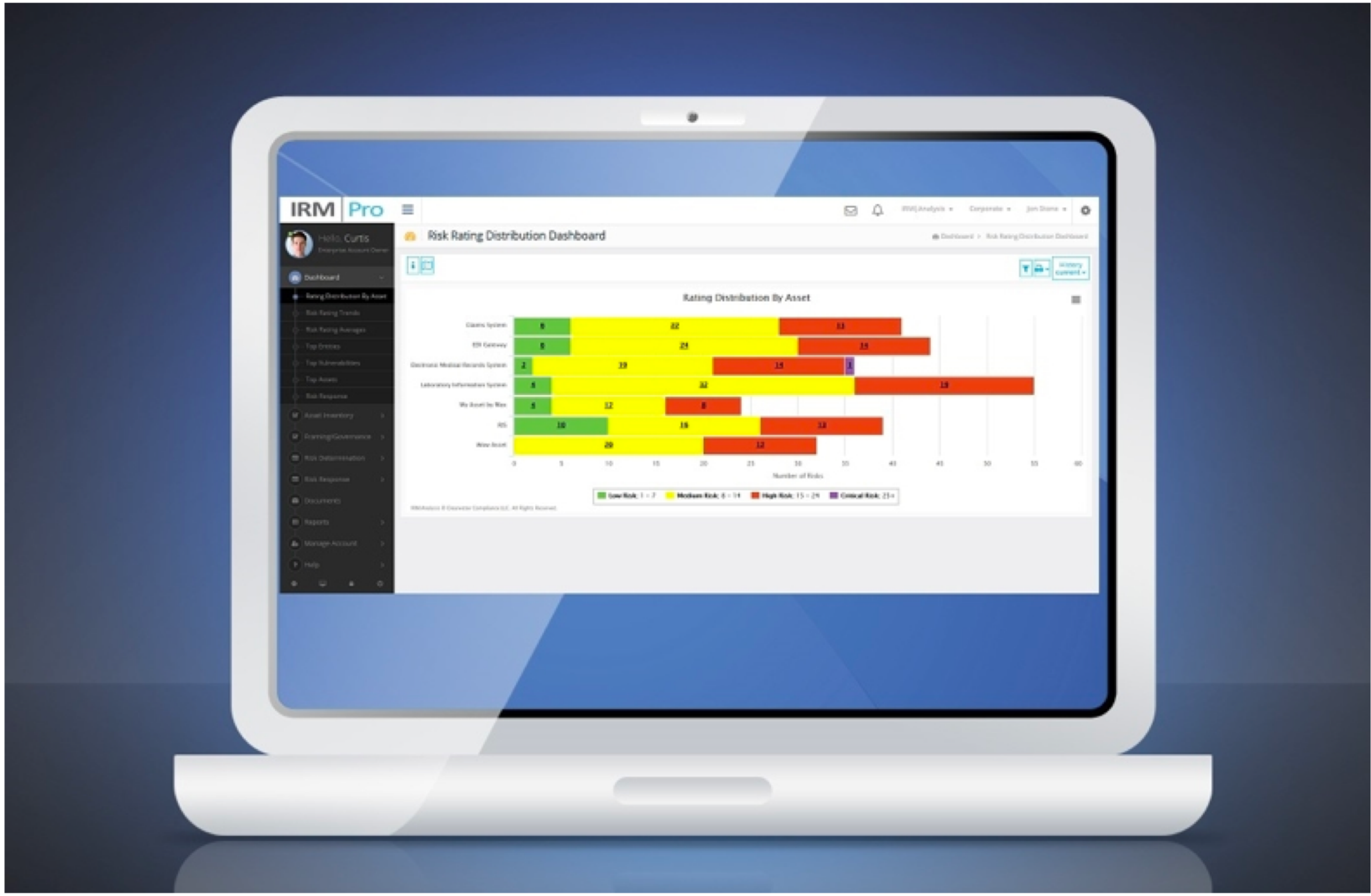
Fortunately things are changing

New Tools and Approaches to TPVRM now exist

Process Automation

Attempting to calculate every threat * vulnerability and every Likelihood * Potential Impact in spreadsheets takes **WAY Too Long** and is prone to inaccurate out of date information like CVEs.

That's why you should be using automated risk assessment tools like IRM Pro to identify and manage HIGH and CRTICAL risks.



IRM Pro
Hello, Curtis
Dashboard
Rating Distribution By Asset
Risk Rating Distribution Dashboard
Rating Distribution By Asset
Claims System
EDI Gateway
Electronic Medical Records System
Laboratory Information System
RIS
New Asset
Number of Risks
Low Risk: 1 - 7
Medium Risk: 8 - 14
High Risk: 15 - 24
Critical Risk: 25+

VIRGINIA Chapter

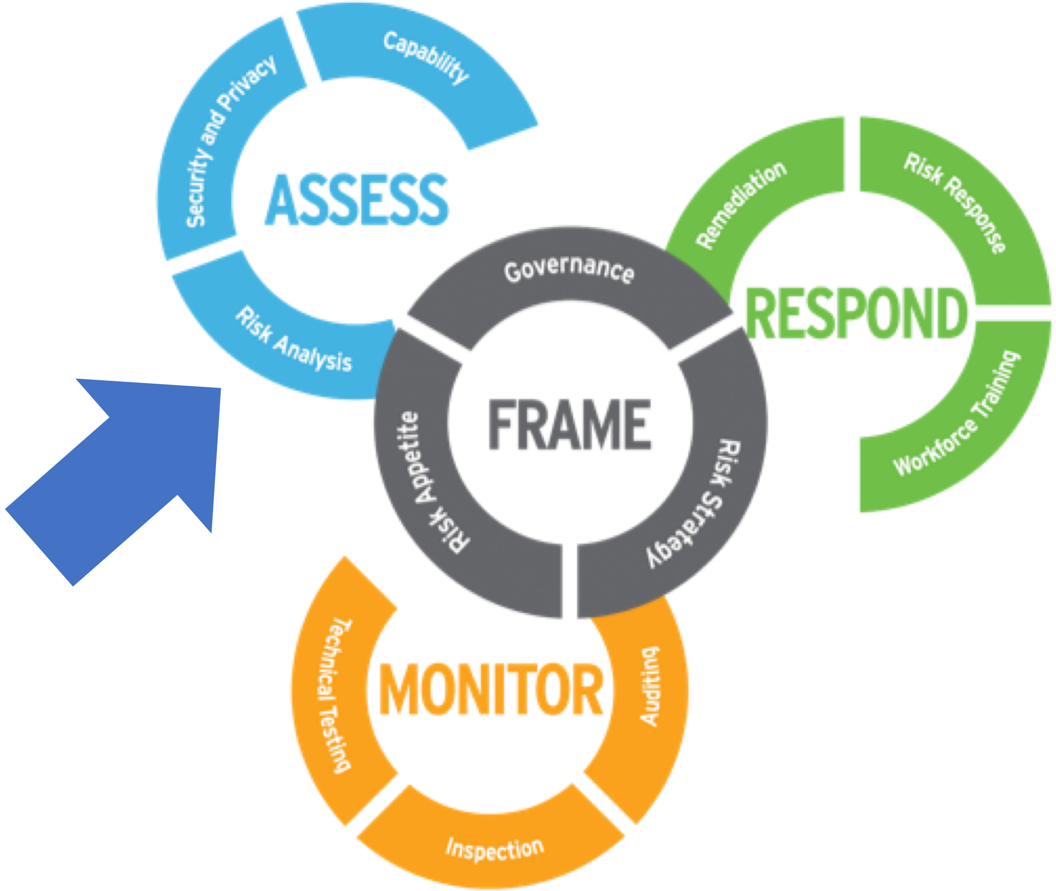
NIST Security Framework

OCR recommends that:

- Risk Analysis follow NIST SP 800-30 standards

- Security controls be evaluated against NIST SP 800-53 standards

- Regardless of the security framework you follow



HIMSS VIRGINIA Chapter

Evidence Sharing Networks

- A relatively new innovation in TPVRM is providing Risk Managers with all of the benefits of the traditional assessment process, but with much less aggravation.
- The advent of Vendor Evidence Sharing Networks is making completed, verified, standard surveys available to organizations while eliminating the tedious time-and-resource consuming process of collecting accurate data from vendors.
- The "**Complete-Once, Share-Many**" model of vendor sharing networks means the burden on vendors is similarly alleviated.
- By greatly reducing the effort required to collect or complete surveys, it means that both first and third parties can spend much less time gathering controls data and much more time on what's important: working together to decrease control gaps and reduce overall risk.

IRM|Pro™: New Product – TPVRM – early 2019

Third-Party Vendor Risk Management

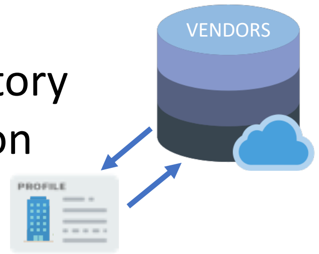
New product to manage the assessment of risk presented by vendors and suppliers

Collaboration

- Assign TPVRM work to internal staff and external vendors
- Monitor progress with work queues, messaging, notifications, reminders

Sole Source of Vendor Risk Information

- Risk ranked vendor and product inventory
- Centralized vendor/product information



IRM|Pro CyberIntelligence™ Dashboards

Monitor and present ***vendor risk management progress*** with full-featured dashboards & reports

Central library of Assessment Information

- Customer created and standards-based assessments (NIST)
- Assessments filled online by vendors and suppliers

Market-leading Features

- Sole source of Vendors Risk Information
- Send assessments based on risk profile
- Automates the workflow and organizes all the moving pieces

Lets not get caught with our pants down people!

HIMSS® VIRGINIA Chapter

Thank You