RSA® Conference 2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID:

RSAConference2020 APJ

A Virtual Learning Experience

Cyber Risk

How do you define cyber risk?

- Risk is the exposure to the possibility of loss, injury, or other adverse or unwelcome circumstance.
- Risk = Uncertainty x Exposure
- Cyber risk is the risk that occurs in digital, wireless, and computer-related activities.

Elements of cyber risk

Cyber risk is related to the use of technology in an organization.

Elements include:

- People
- Process
- System
- External events

Cyber risk is very important nowadays as cyber threats target all kinds of organizations and government entities.

Black Swan events can happen

BLACK SWAN RISKS ARE RARELY OCCURRING RISKS THAT ARE MUCH MORE DIFFICULT TO MANAGE AND MEASURE.

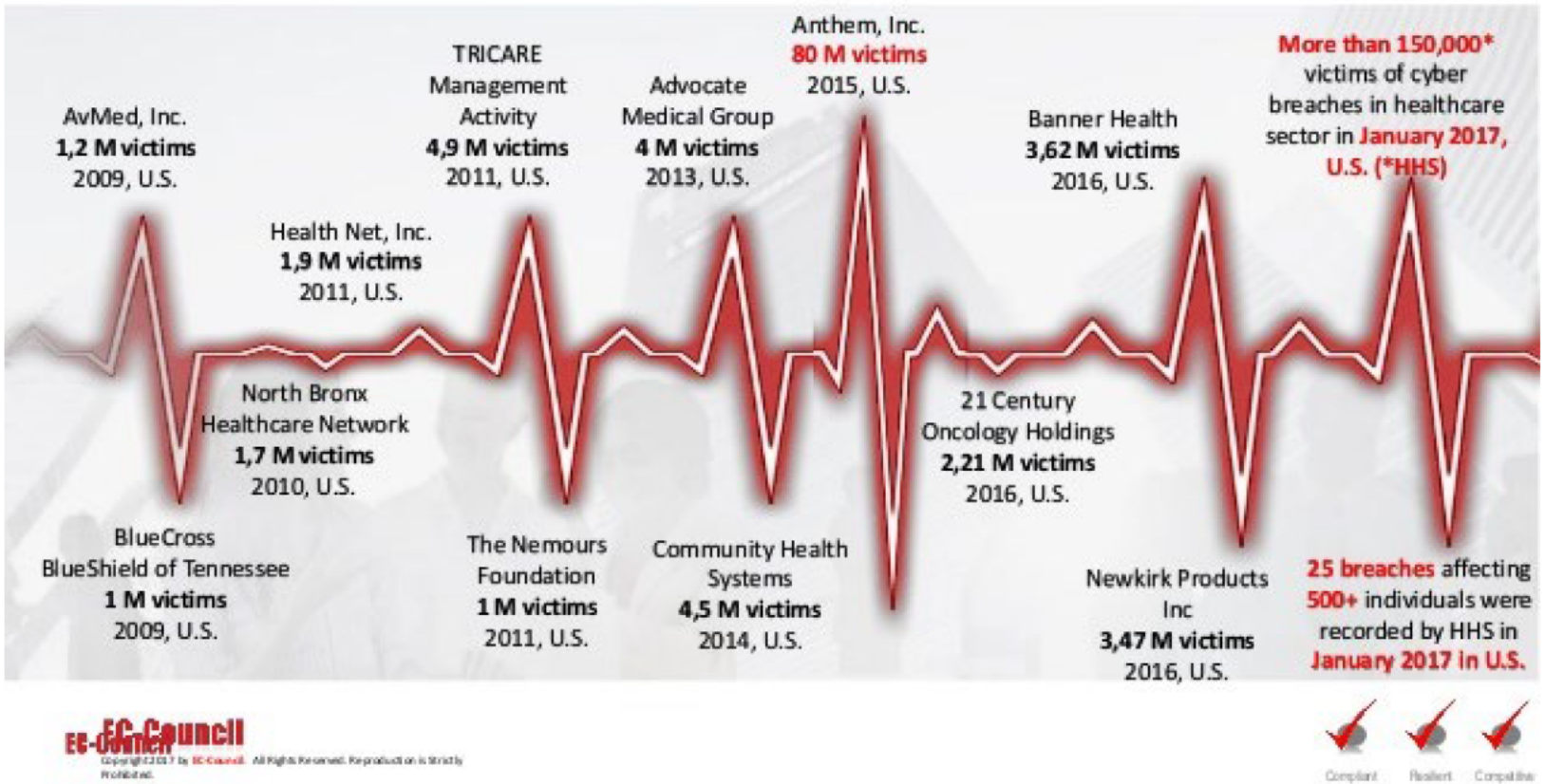
The Electric Company
El Paso Electric

Cyber Risk in Financial Services

Risk.net survey results

2016	2017	2018
#1 Cyber risk	#1 Cyber risk and data security	#1 IT disruption
#2 Conduct risk	#2 Regulation	#2 Data compromise
#3 Regulation	#3 Outsourcing	#3 Regulatory risk
#4 AML, CTF and sanctions compliance	#4 Geopolitical risk	#4 Theft and fraud
#5 Organizational change	#5 Conduct risk	#5 Outsourcing
#6 Outsourcing	#6 Organizational change	#6 Mis-selling
#7 Recruitment and retention	#7 IT failure	#7 Talent risk
#8 IT failure	#8 AML, CTF and sanctions compliance	#8 Organizational change
#9 Terrorism	#9 Fraud	#9 Unauthorized trading

Cyber Risk in Healthcare



The Electric Company
El Paso Electric

RSAConference2020 APJ
A Virtual Learning Experience

Cyber Risk in the energy sector

The Electric Company
El Paso Electric

RSAConference2020 APJ
A Virtual Learning Experience

Cybersecurity events in the last two decades

Cyber Activities

In cyberspace, a few lines of malicious code can be written (or purchased on the dark web) by any number of state or nonstate actors to damage network systems.

In most cases, hackers can be classified into three major groups. Activists or hacktivists, profit-seekers, and nation-state sponsored.

The three main vectors of cyberattacks

Sophisticated attackers often use:

- Interconnected network systems.
- Human insiders (malicious or careless)
- The supply chain

Major Cyber Attacks since 2010

- In 2010 the Stuxnet virus attacks that led to the destruction of more than 1,000 Iranian centrifuges and delayed Iran's enrichment program was widely attributed to the United States and Israel.
- Some analysts believe that denial-of-service attacks that disrupted U.S. financial institutions in 2012 and 2013 were launched by Iran in retaliation for the Stuxnet attacks.
- In 2012 many blamed Iran for the "Shamoon" virus attacks that destroyed some 30,000 computers belonging to the Saudi Aramco Corporation.

Major Cyber Attacks

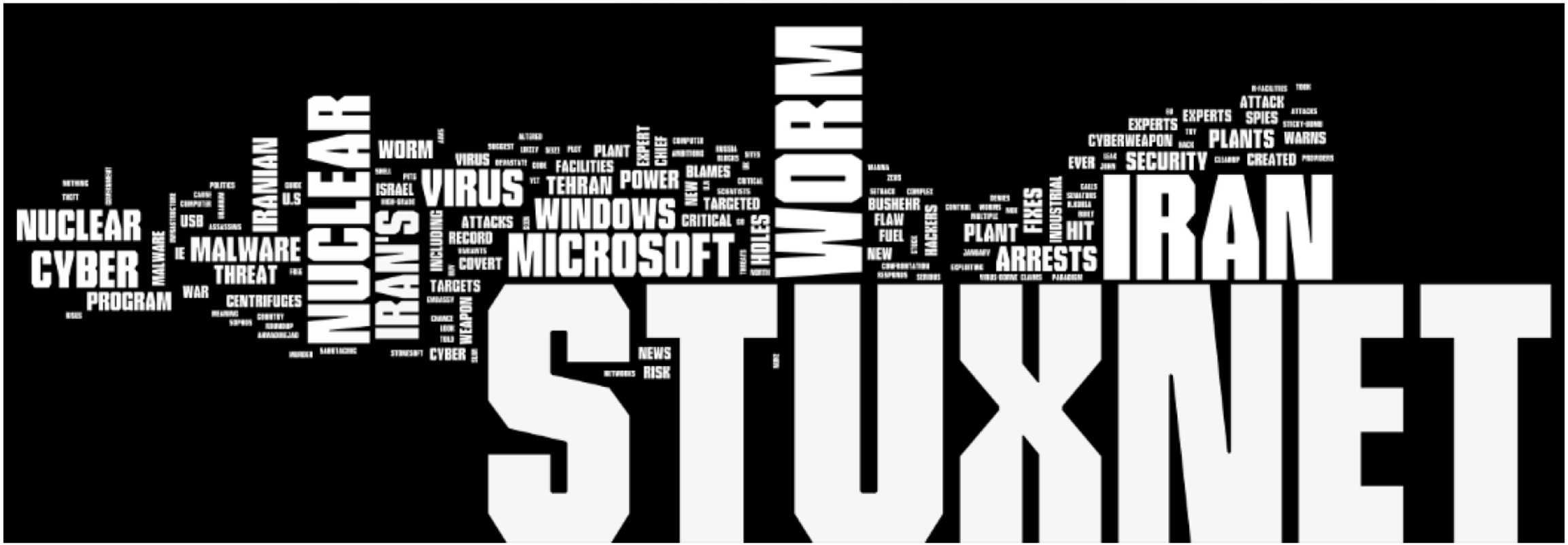
- North Korea frequently penetrated and disrupted South Korean networks.
- In 2014, North Korea caused damage to machines, data, and reputations at Sony Pictures in the United States.
- In December 2015, externally introduced malware caused a three- to six-hour interruption for some 225,000 users of the Ukrainian electrical grid.

RSAConference2020 APJ

A Virtual Learning Experience

Stuxnet

Stuxnet Case



MALWARE CODE RUNNING IN COMPUTERS THAT CONTROLLED THE INDUSTRIAL SYSTEMS AT THE NUCLEAR PLANT

The Electric Company
El Paso Electric

Stuxnet Case

- In January 2010, the Natanz nuclear enrichment plant in Iran experienced unexplained explosions of the centrifuges used to enrich uranium.
- This was the second time the nuclear plant had problems with the centrifuges as they had experienced manipulation of the valves and damages to the devices back in 2019.
- In June 2010, a group of researchers in Belarus found malware code running in computers that controlled the industrial systems at the plant.

Stuxnet Case

- It was discovered that earlier versions of the malware were released since 2009 and the developers of this cyber weapon improved it to make it the most sophisticated virus ever developed.
- The code targeted Programmable Logic Controllers (PLCs) manufactured by the German firm, *Siemens*. PLCs are computer devices physically attached to industrial control systems.
- The Siemens S7-4000 PLCs targeted by this malware manipulated the frequency converters that altered the operational speed of the centrifuges and made them fail.

Attack Phases

- First, the cyber actors obtained intelligence from different sources and identify the specific models of the PLCs that were directly controlling the centrifuges.
- With the information in hand, the attackers started the development of the malware.

Attack Phases

- Once the malware was created, the attackers spent quite some time in the delivery phase. At this point, there was interaction with contractors who were known to connect their computers to systems in the nuclear plant.
- Finally, once the virus infiltrated the systems it started the exploitation phase by carefully running the code that made the centrifuges fail.

Security Controls in Industrial Control Systems

- Most of the PLCs and similar devices categorized as Industrial Control Systems (ICS) lack security controls and are very easy to manipulate.
- The PLCs hold a unique identifier and the malware only infected the specific models that were needed for the attack.
- Once the PLCs were compromised, the malware tested the uranium enrichment process and eventually changed the speed on the devices. The program was blowing up centrifuges and leaving no trace.

The Electric Company
El Paso Electric

Third-Party Vendors compromised

- A major weakness was the lack of security controls for contractors and third-party vendors.
- The attacker knew whom to infect first, with the help of infiltrated people who helped obtain genuine digital certificates.
- Three main contractors were infected, and the virus propagated using USB flash drives that were not sanitized or scanned for malware before using them.

The Electric Company
El Paso Electric

RSAConference2020 APJ

A Virtual Learning Experience

Managing the risk

Risk Management

Risk can be managed by reducing:

- Uncertainty (probability of event happening) or
- Exposure of critical information or information systems

What are many energy organizations doing?

Cybersecurity Capability Maturity Model (C2M2)

The **Cybersecurity Capability Maturity Model** (C2M2) program is a public-private partnership effort that was established as a result of the Administration's efforts to improve electricity subsector **cybersecurity capabilities**, and to understand the **cybersecurity** posture of the grid.

The Electric Company
El Paso Electric

C2M2

- Developed at Carnegie Mellon
- Actively used in the power industry
- Focuses on the implementation of cybersecurity practices associated with informational technology (IT) and operational technology (OT) assets
- Considers organization's approach to the ten domains and management objectives to becoming a mature organization
- Includes the Maturity Indicator Level (MIL) for the 10 domains

The Electric Company
El Paso Electric

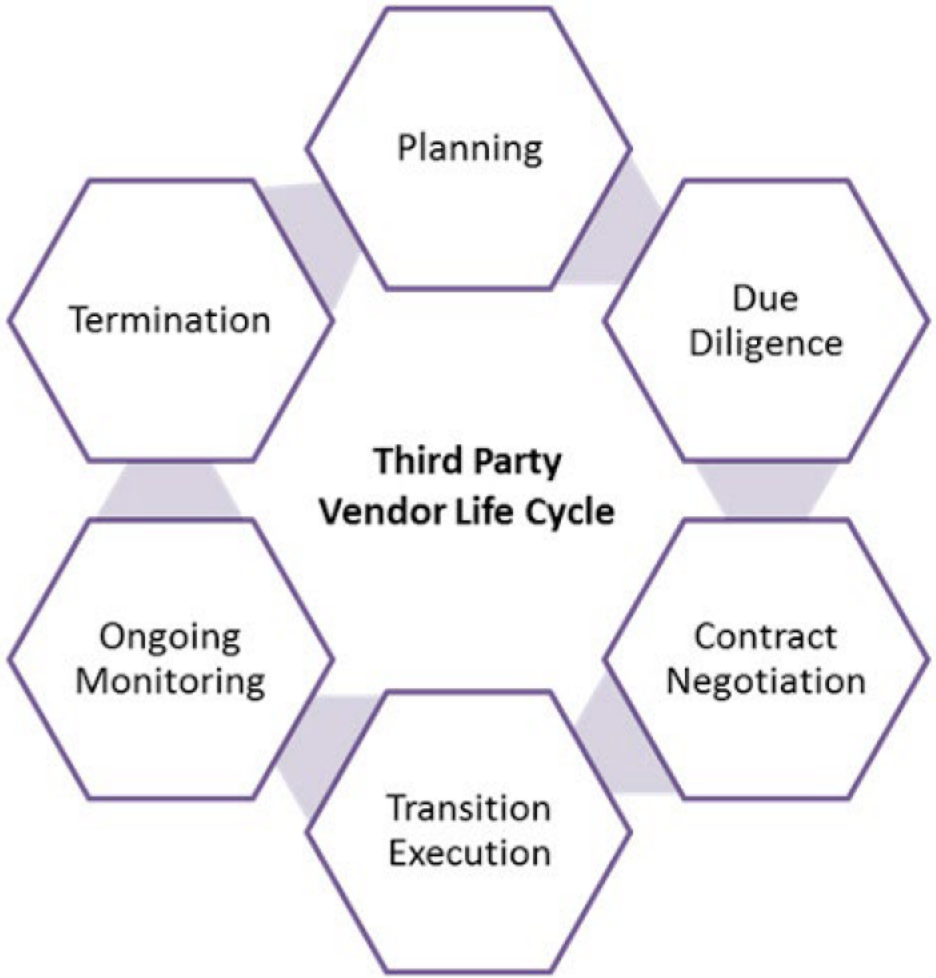
1. Risk management
2. Asset change and configuration management
3. Identity and access management
4. Threat and vulnerability management
5. Situational awareness
6. Information sharing and communications
7. Event and incidents response and continuity of operations
8. Supply chain and external dependencies
9. Workforce management
10. Cybersecurity program management

RSAConference2020 APJ

A Virtual Learning Experience

Third Party Risk Management (TPRM)

Third Party Risk Management



The Electric Company
El Paso Electric

Third Party Risk Management

Building new digital relationships with third-parties increases exposure to a cybersecurity breach. But by following the right path IT leaders can feel confident in their approach to managing the cyber risk of these relationships.

The Electric Company
El Paso Electric

Vendor Relationships

Every company today finds itself part of a digital data web along with its partners, vendors, and other third-party organizations.

The Electric Company
El Paso Electric

What to do

- Employing network security measures, such as *air gaps*, can ensure secure computer networks are physically isolated from unsecured networks. However, this can be a challenge in some cases because there are not any truly air-gapped networks in production environments. They still need code upgrades, log files, upgrade equipment, computers, etc.
- It is very important to have a vendor risk assessment program in place and comply with standards to protect critical infrastructure.

The Electric Company
El Paso Electric

TPRM

- Many companies don't know how to initiate such a program, much less optimize and maintain it.
- Managing Third-Party Risk to protect the value of the organization could be challenging.
- There are software tools that can automate the process and make it more efficient.

TPRM Tools

Third Party Risk Management tools help to:

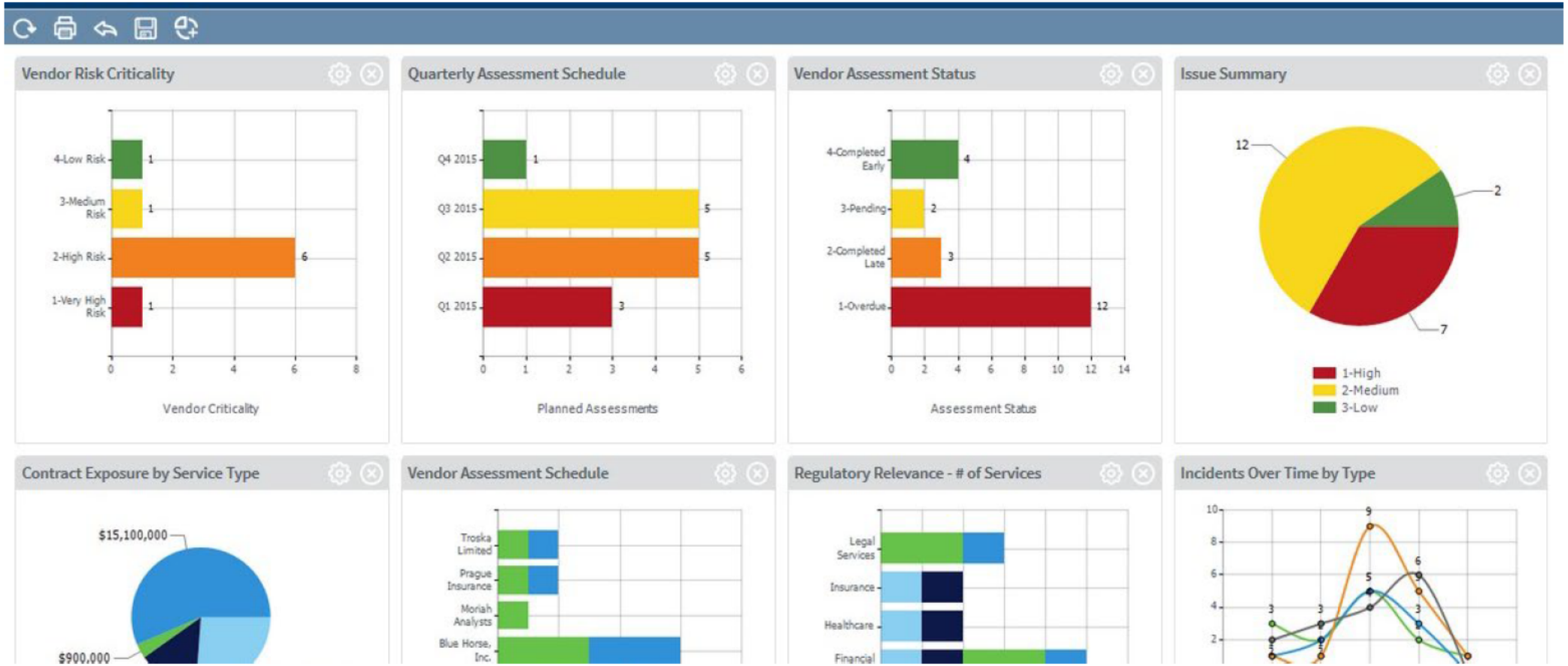
- Move from a manual to an automated process
- Expand the number of vendors being assessed
- Align with Enterprise Vendor Management programs
- Provide visibility in dashboards
- Easy reporting to executive management

The Electric Company
El Paso Electric

TPRM Tools


VENDOR DASHBOARD
Infosec Vendor Risk Rating
1. Critical
2. High
3. Medium
4. Low
5. No Risk Rating
Vendor
Infosec Vendor Criticality
1. Critical
2. High
3. Medium
4. Low
5. No Criticality
Vendor
Vendor Type
Consulting
Contract
Hosting
Software
Vendor Type
Vendor Assessment Schedule
Current
Q3 2020
Assessment Status 2018
2. With Respondent / Working
4. Submitted, In Review
5. Assessment Complete
Vendor Owner
Supply Chain Management
Information Security

TPRM Tools



The Electric Company
El Paso Electric

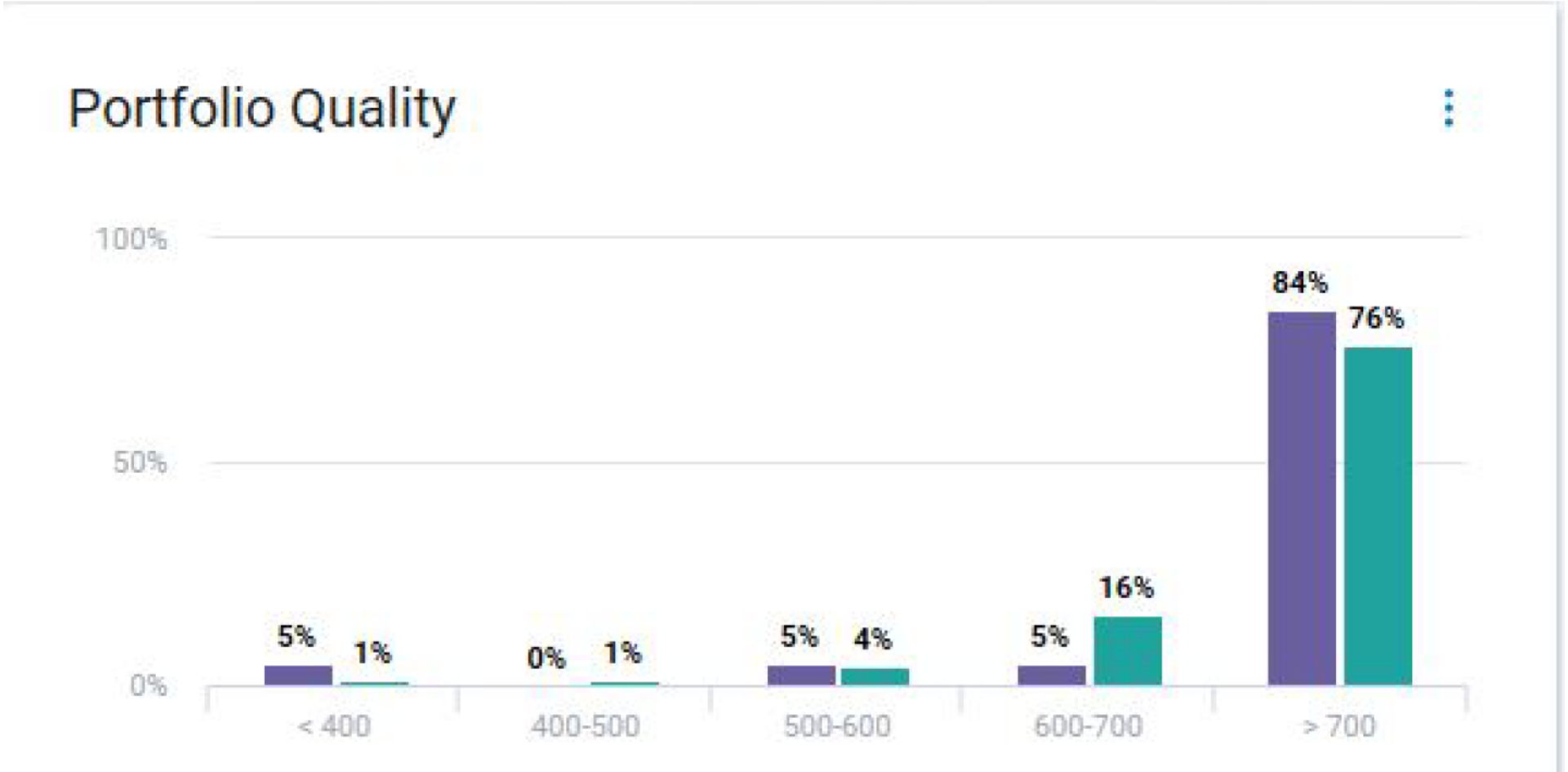
RSAConference2020 APJ
A Virtual Learning Experience

TPRM Tools

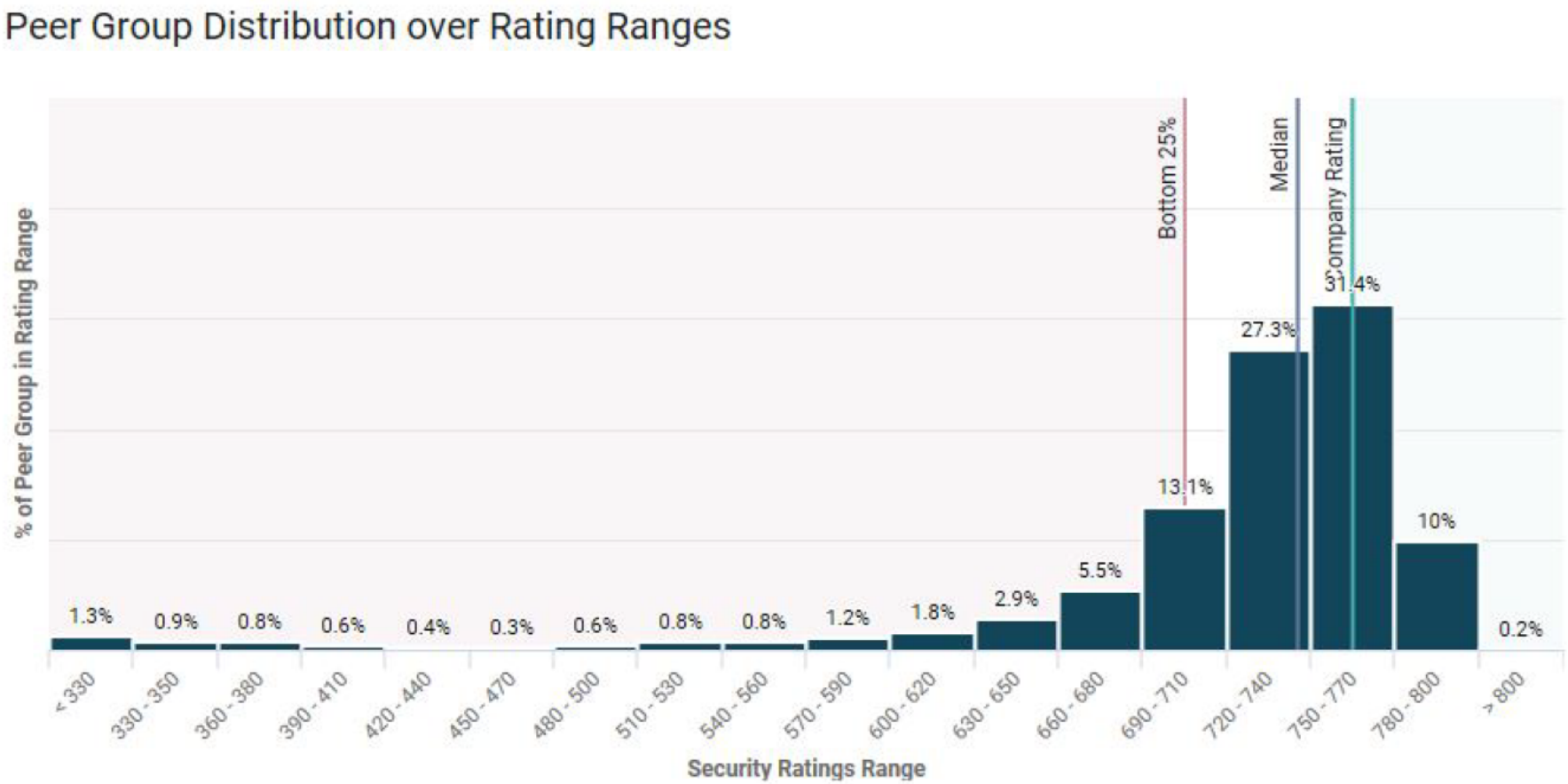
		expose Company's intellectual property.				
	Customer alienation	Vendor may alienate Company's customers.	6/10/2014	Kyle Brown	High	Medium
	Vendor financial failure	Vendor may suffer a financial failure.	6/10/2014	Kyle Brown	High	High
	Damage to reputation	Vendor may damage Company's reputation.	6/10/2014	Kyle Brown	Very High	Medium
	Code of Ethics violation	Vendor may violate Company Code of Ethics.	6/10/2014	Kyle Brown	High	Medium
Troska Limited						
	2014 Troska Risk Review					
	Vendor Risks					
	Failure to deliver	Vendor may fail to deliver on contract.	6/10/2014	Keith Brady	Very High	High
	Data breach risk	Vendor may suffer a data breach.	6/10/2014	Keith Brady	Very High	High
	Loss of Company IP	Vendor may appropriate or inadvertently expose Company's intellectual property.	6/10/2014	Keith Brady	High	Low
	Customer alienation	Vendor may alienate Company's customers.	6/10/2014	Keith Brady	High	Medium
	Vendor financial failure	Vendor may suffer a financial failure.	6/10/2014	Keith Brady	High	High

The Electric Company
El Paso Electric

TPRM Tools


Portfolio Quality
100%
50%
0%
5%
1%
0%
1%
5%
4%
5%
16%
84%
76%
< 400
400-500
500-600
600-700
> 700

TPRM Tools



The Electric Company
El Paso Electric

TPRM Tools

The Electric Company
El Paso Electric

TPRM Program

Small, medium, or large, every company needs a TPRM program that matches its specific circumstances and available resources.

Many companies are just at the initial stages of designing and launching such a program.

Others have TPRM programs that rely too heavily on subjective vendor self-assessments, or other point-in-time evaluations.

TPRM Program

Organizations need continuous visibility into all of the third parties it trusts with sensitive information and access.

Only by having such a comprehensive and consistent TPRM approach can organizations hope to both identify potential third-party vulnerabilities as well as fairly compare one organization's risks with those of alternative vendors and partners.

The Electric Company
El Paso Electric

Recommendations

- Continuously updated ratings
- Constant communication with vendors
- Testing environments with built–in analysis tools
- Detect and correct any shortcomings
- In some cases replace vendors with more trustworthy third parties

Goals of TPRM: Mitigate Risk

Reduce our risk of non-compliance and reduce the risk of reportable incident by:

- Continuously monitoring vendor performance (more efficiently)
- Systematically enforcing company third-party risk policies
- Improving vendor coverage and monitoring capabilities

The Electric Company
El Paso Electric

Goals of TPRM : Eliminate Surprises

Increase organizational/management awareness and visibility of our vendor risk profile by:

- Increasing visibility to risk and its impact to the organization
- Ensuring accountability through a comprehensive program

Goals of TPRM : Reduce Operating Costs

Reduce compliance costs both internally and externally by:

- Consolidating and streamlining compliance activities
- Lowering the cost per vendor assessment
- Streamlining reporting and audit support

The Electric Company
El Paso Electric

End Goal: Preventing the next attack

Action Plan

Immediate actions:

- Identify all the critical assets of your organization
- Identify all vendors and create different tiers to group them
- Establish security controls that are aligned with TPRM

Action Plan

In the first three months following this presentation you should:

- Select the tools that best suit your needs
- Choose how to assess the different vendors
- Develop a schedule to run the assessments
- Send the assessment to your vendors

Action Plan

Within six months you should:

- Communicate with vendors regarding weak security controls in their systems/processes and work with them on remediation
- Be prepared to replace vendors that do not comply with your security standards

RSAConference2020 APJ

A Virtual Learning Experience

Rafael Garcia

@rafuca