IDC | ANALYZE THE FUTURE

The State of Midsize Enterprise Cybersecurity

Pete Lindstrom
VP of Security Strategies

The State of Midsize Enterprise Cybersecurity

9/18 9am-9:15am

In today's digital world, data breaches seem like a fact of life. Having payments fraudulently re-routed, leaking customers' private information, and enabling – or being accused of enabling – nation-state attacks of critical infrastructure are all very real risks to midsized enterprises. And these enterprises are more likely to experience unrecoverable damage leading to bankruptcy or worse. Let's take a quick look at results from our cybersecurity survey regarding the things that you and your peers have identified as the key risks, challenges, and controls associated with your cybersecurity programs.

Pete Lindstrom

Vice President, Security Strategies
IT Executive Program, IDC

- Over 25 years in InfoSec, IT, Finance
- Tech Risk Pro performing reading, writing, ‘rithmetic on risk and security matters
- Former Marine (Gulf War veteran), ‘Big Four’ IT Auditor (PwC), Internal Auditor (GMAC Mortgage), Security Architect & Director (Wyeth)
- BBA Finance, University of Notre Dame; former CISSP and CISA

THE WALL STREET JOURNAL.

ILLUSTRATION BY JESSICA KURONEN/WSJ

America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It

A Wall Street Journal reconstruction of the worst known hack into the nation's power system reveals attacks on hundreds of small contractors

By *Rebecca Smith* and *Rob Barry*

Jan. 10, 2019 11:18 am ET

THE WALL STREET JOURNAL.

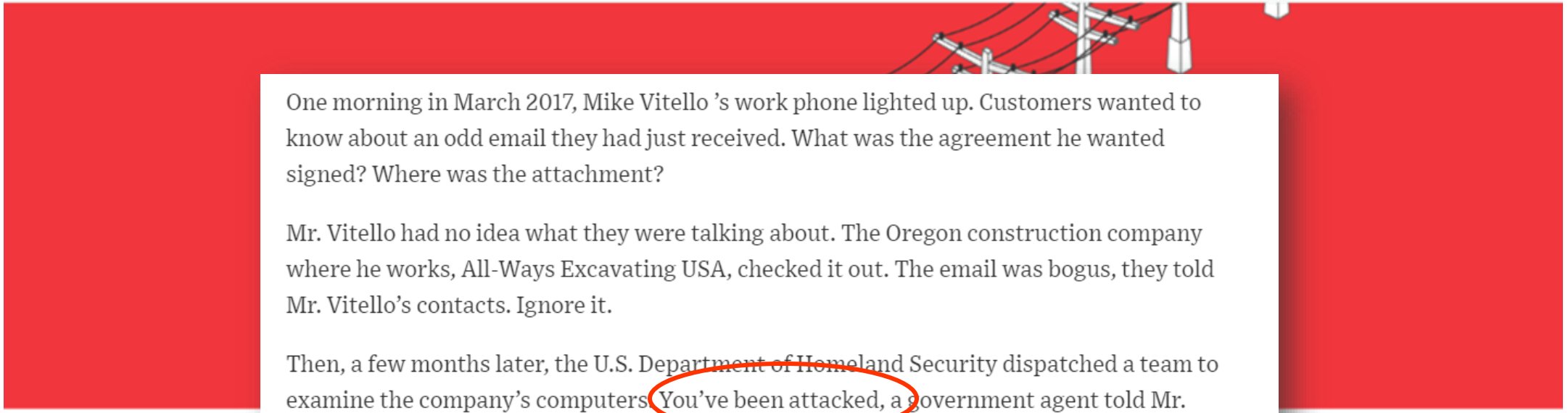


ILLUSTRATION BY JE

Americ ...oor—and

A Wall Street ... ...tem reveals attacks

By *Rebecca Smith* and *Rob Barry*

Jan. 10, 2019 11:18 am ET

One morning in March 2017, Mike Vitello 's work phone lighted up. Customers wanted to know about an odd email they had just received. What was the agreement he wanted signed? Where was the attachment?

Mr. Vitello had no idea what they were talking about. The Oregon construction company where he works, All-Ways Excavating USA, checked it out. The email was bogus, they told Mr. Vitello's contacts. Ignore it.

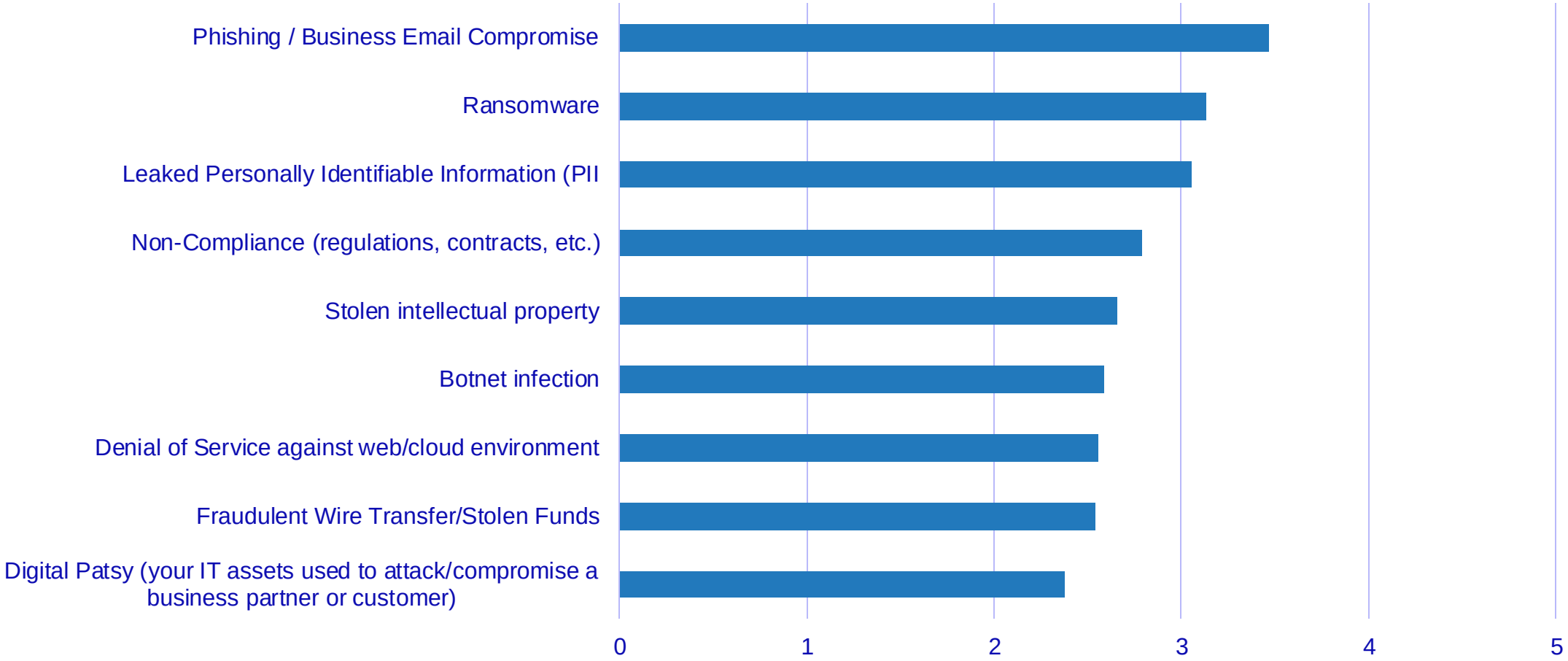
Then, a few months later, the U.S. Department of Homeland Security dispatched a team to examine the company's computers. You've been attacked, a government agent told Mr. Vitello's colleague, Dawn Cox. Maybe by Russians. They were trying to hack into the power grid.

"They were intercepting my every email," Mr. Vitello says. "What the hell? I'm nobody."

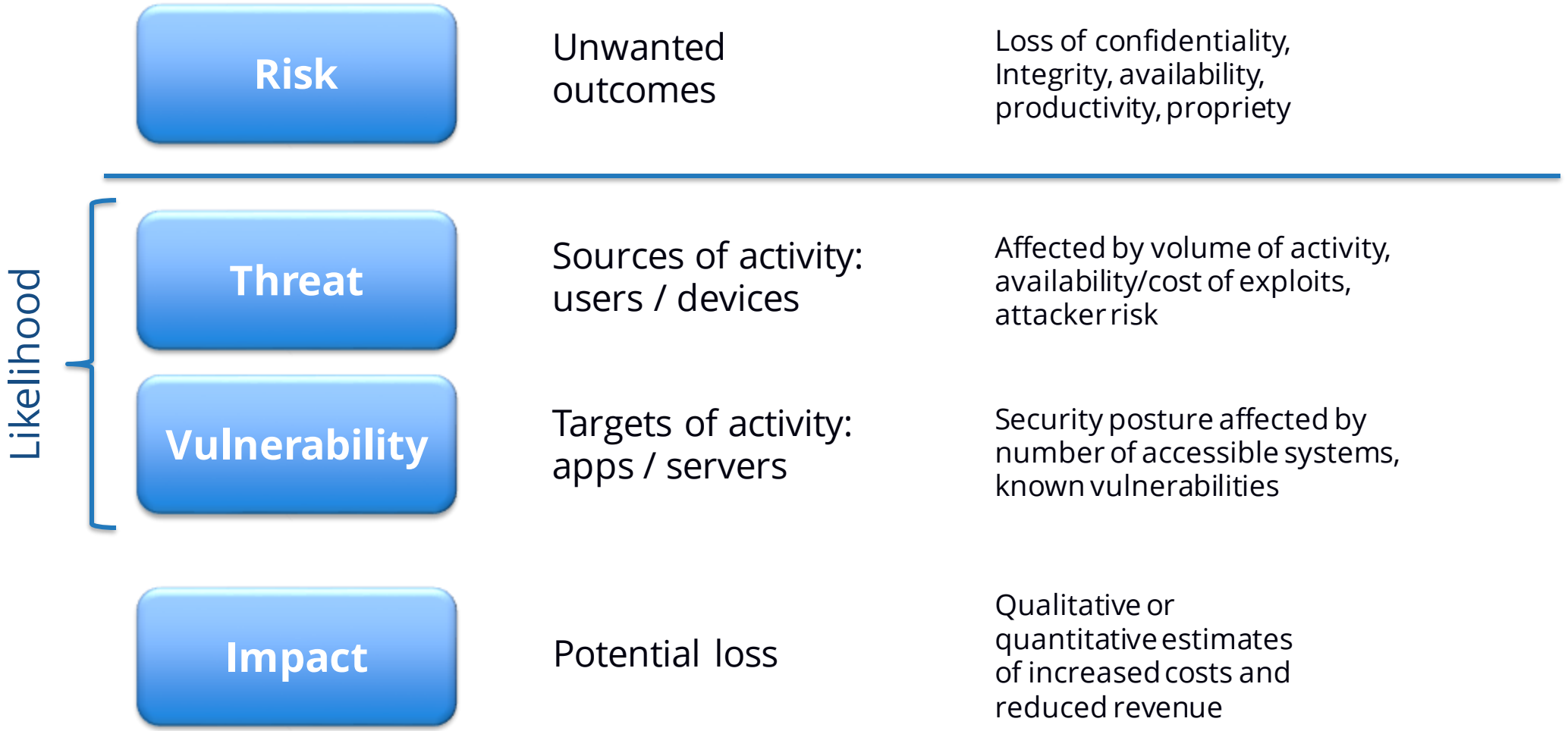
"It's not you. It's who you know," says Ms. Cox.

The cyberattack on the 15-person company near Salem, Ore., which works with utilities and government agencies, was an early thrust in the worst known hack by a foreign government into the nation's electric grid. It set off so many alarms that U.S. officials took the unusual step in early 2018 of publicly blaming the Russian government.

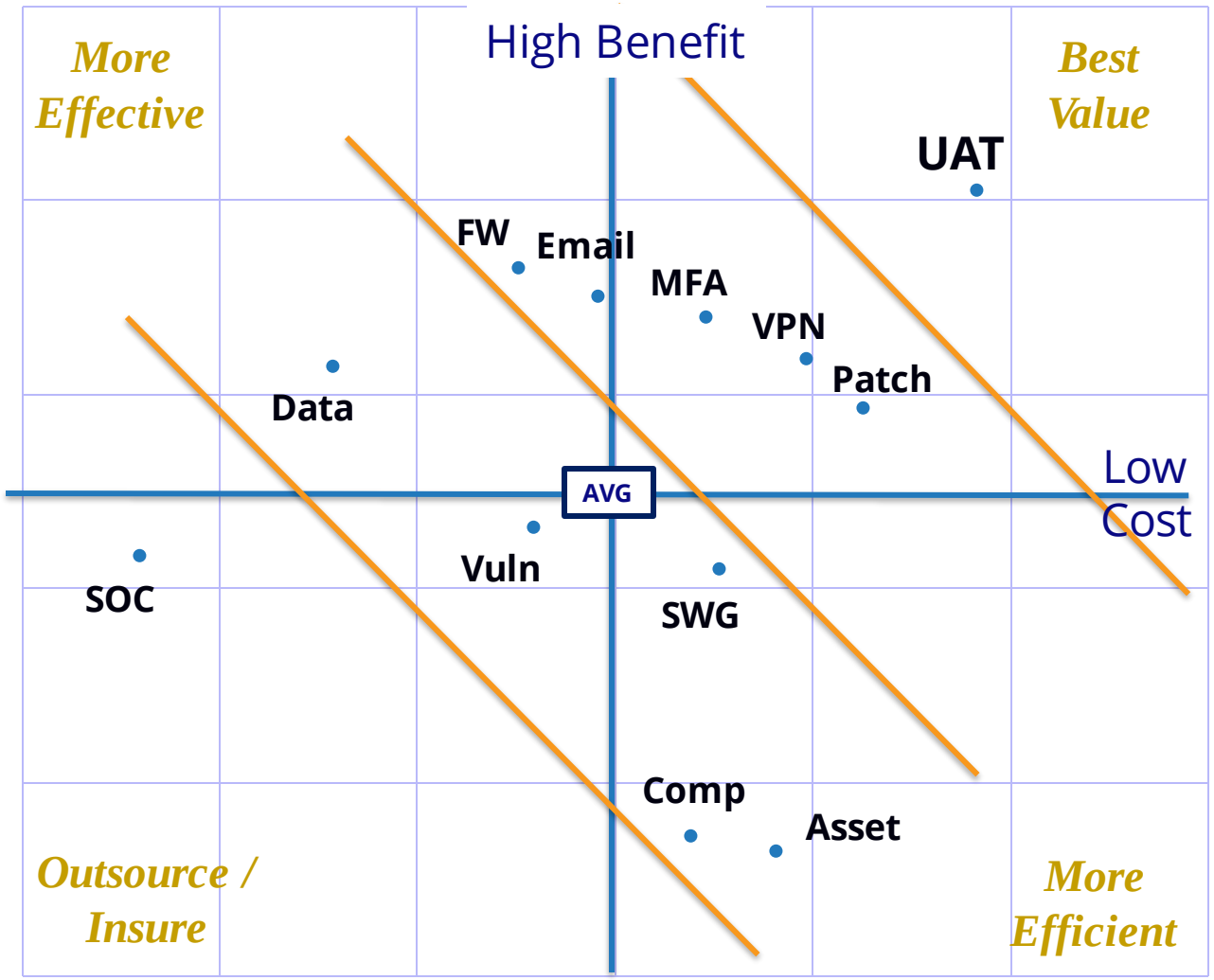
MES Survey: What are your top risks?



The Components of Risk



MES Survey: What are your best controls?



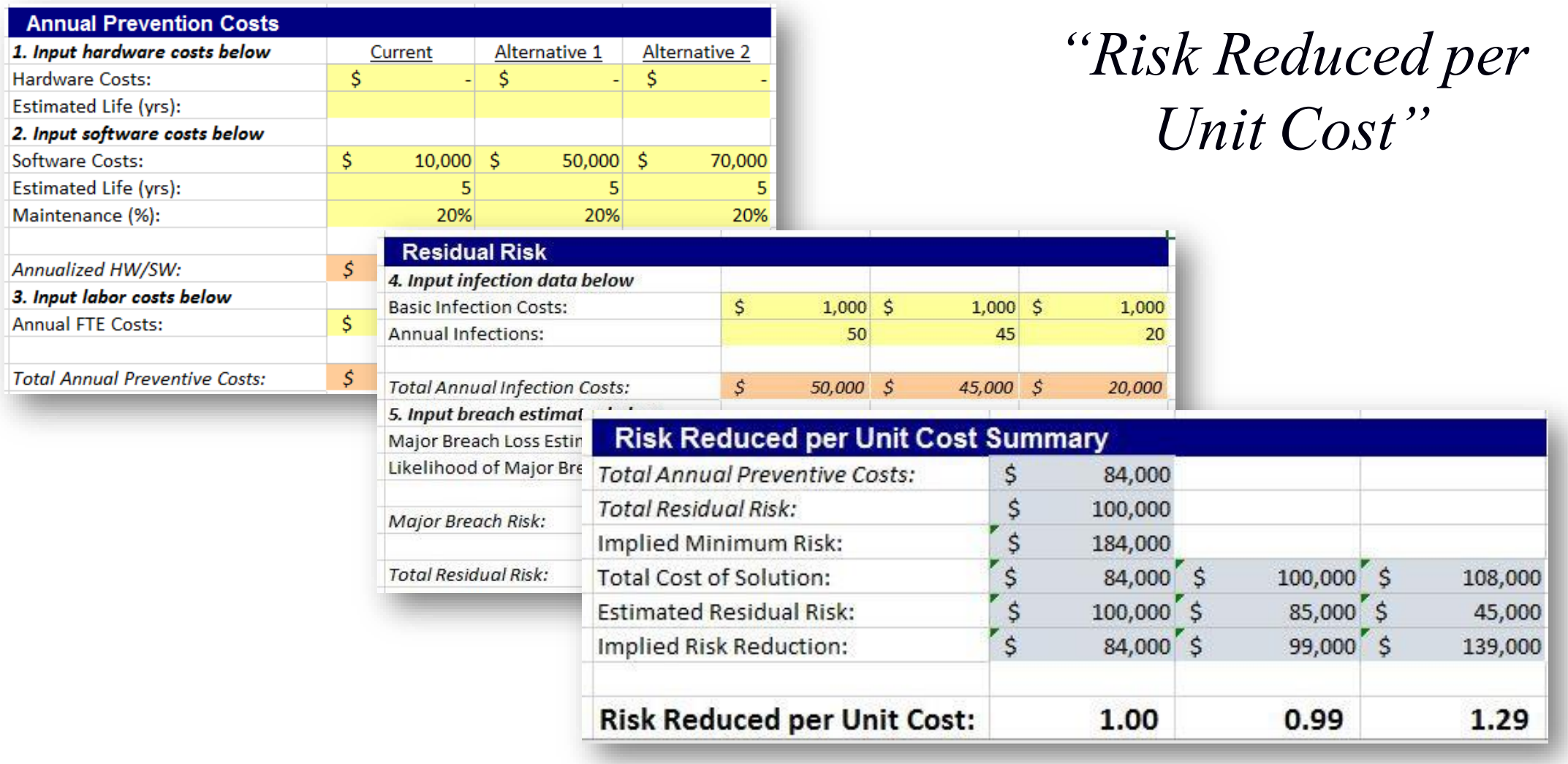
UAT: User awareness training

Patch: Patch management
VPN Encrypted communications
MFA: Multifactor authentication
Email: Email security solutions
FW: Firewalls

SWG: Secure web gateways / proxies
Vuln: Vulnerability scanning
Data: Data security
Asset: Asset/config management
Compliance: Compliance activities

SOC: Security operations center

In Search of… Economic Analysis for RRUC



Annual Prevention Costs			
1. Input hardware costs below	Current	Alternative 1	Alternative 2
Hardware Costs:	$ -	$ -	$ -
Estimated Life (yrs):			
2. Input software costs below			
Software Costs:	$ 10,000	$ 50,000	$ 70,000
Estimated Life (yrs):	5	5	5
Maintenance (%):	20%	20%	20%
Annualized HW/SW:	$		
3. Input labor costs below			
Annual FTE Costs:	$		
Total Annual Preventive Costs:	$		

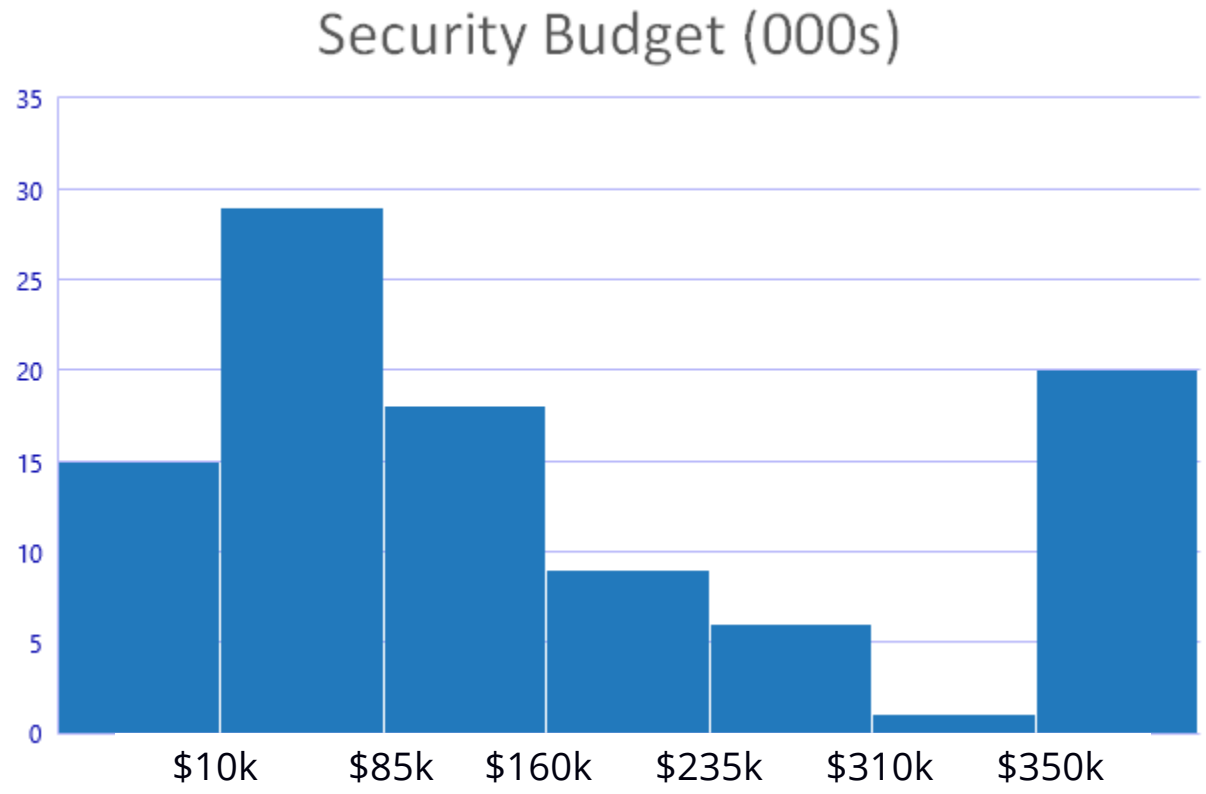
Residual Risk			
4. Input infection data below			
Basic Infection Costs:	$ 1,000	$ 1,000	$ 1,000
Annual Infections:	50	45	20
Total Annual Infection Costs:	$ 50,000	$ 45,000	$ 20,000
5. Input breach estimat			
Major Breach Loss Estin			
Likelihood of Major Bre			
Major Breach Risk:			
Total Residual Risk:			

Risk Reduced per Unit Cost Summary			
Total Annual Preventive Costs:	$ 84,000		
Total Residual Risk:	$ 100,000		
Implied Minimum Risk:	$ 184,000		
Total Cost of Solution:	$ 84,000	$ 100,000	$ 108,000
Estimated Residual Risk:	$ 100,000	$ 85,000	$ 45,000
Implied Risk Reduction:	$ 84,000	$ 99,000	$ 139,000
Risk Reduced per Unit Cost:	**1.00**	**0.99**	**1.29**

"Risk Reduced per Unit Cost"

MES Survey: What are your spending plans?

MES Survey: How much are you spending?



Scarce Resources ***High Expectations***

Peers: Best Practices for Security Budgets

Your Challenges	Peer Insights
An annual budget and risk audit stymies the ongoing remediation of new and ever-evolving security threats.	**Practice 1: Implement a standard, continuous process to identify threats, measure risk, and fix vulnerabilities.**
Increasing hyper-connectivity equals greater risk exposure, driving up costs.	**Practice 2: Use a trusted network of security sources inside and outside of IT and your own industry.**
Recruiting and retaining experienced security professionals as employees is more difficult and costly in the face of security skills shortages.	**Practice 3: Consider security skills shortages and future operating costs when making security outsourcing decisions.**
IT executives must educate boards of directors about cybersecurity risks and the cost of protection.	**Practice 4: Gear security budget presentations to business outcomes when addressing senior executives and the board.**

Throughout the day…

- Look for ways that help you ASSESS RISK
- Look for ways that help you APPLY CONTROLS
- Look for ways that help you ALLOCATE RESOURCES

And never forget…

The Cybersecurity Mission Statement

*"To enable **business transformation** through proper cyber risk management by allocating security resources **efficiently** and **effectively** leading to the strongest cybersecurity program possible."*

IDC is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For more than 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.