RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SEM-01

Information Security Leadership Development: Surviving as a Security Leader

MODERATOR: **Evan Wheeler**

Executive Director, Operational Risk Management
DTCC

PANELISTS:

Bruce Bonsall
Principal Consultant
Bruce Bonsall LLC

JB Rambaud
Managing Director
Stroz Friedberg LLC

Julie Fitton
Chief Information Security Officer
EMC Cloud Services

Malcolm Harkins
Global CISO
Cylance Corporation

#RSAC

Information Security Leadership: Surviving as a Security Leader

Start Time	Title	Presenter
8:30 AM	First 6 Months on the Job	Bruce Bonsall
9:15 AM	Cyber Security in the Boardroom	Malcolm Harkins
10:00 AM	BREAK	
10:15 AM	The Long Walk to the CEO's Office	JB Rambaud
11:00 AM	Reflecting on the Next Generation CISO	Evan Wheeler, Bruce Bonsall, Malcolm Harkins, Julie Fitton, JB Rambaud

RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SEM-M01

Surviving as a Security Leader: First 6 Months on the Job

Bruce Bonsall, CISSP
Principal Consultant
Bruce Bonsall LLC
@brucebonsall

#RSAC

The First 6 Months on the Job

20 days	60 days	40 days
Cultural Assimilation		
	Assess business model, regulatory obligations, global threats, specific threats, infrastructure, current security posture, people, processes	
		Perform Gap Analysis, Design Strategic Roadmap

Show Leadership

Assert Yourself!

There's a New Sheriff in Town!!

Culture

Inertia

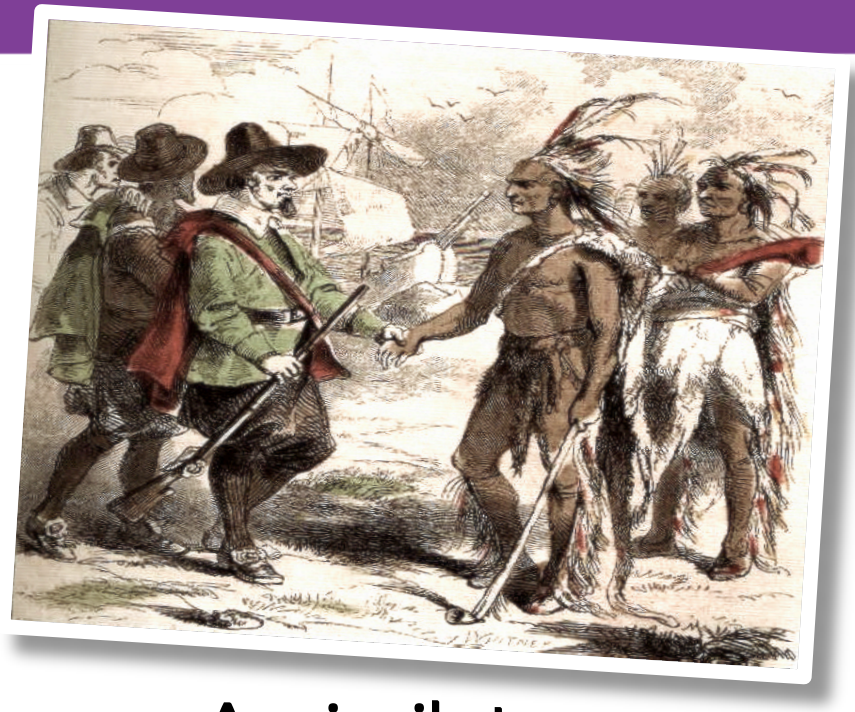
..or maybe not

Do NOT Underestimate the Significance of Organizational Culture

First Impressions Count!

Get Out of My Office!

Welcome to the New World



Assimilate

Beer!

Diplomacy

Diplomacy

Defined as:

the ability
to deal with people
in a sensitive
and effective way

Sensitive: Having or displaying a quick and delicate appreciation of others' ***feelings***

Effective: Successful in producing a **desired** or intended **result**

Ask for More Than You Expect to Get

- Henry Kissinger said when speaking of international negotiation, your ability to get what you want depends on your ability to overstate demands.

  There are several reasons for overstating your demands:
  - You might actually get it
  - It raises the imputed/perceived value of what you're offering
  - It's easier to negotiate (down) to what you really want
  - It can prevent deadlocks with someone who always needs to *win*

Build Credibility

Form Alliances

Clarify Business Challenges with Key Business and IT Leaders

Information Security is a BUSINESS Issue!

Survey the Organization's Risk Landscape

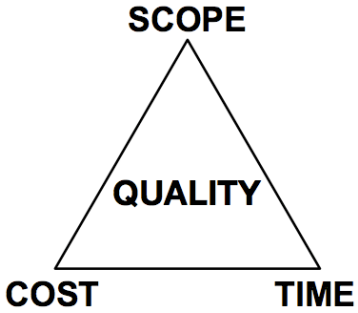
Hunting for Treasures

Where to find information about the organization's information systems

Security Information Management requires a sort of sheepdog mentality

You need to take inventory ….often

Organization-Specific Concerns



Click Jackers

NIST

HACKERS

PCI DSS

FERC

HIPAA

FISMA

GLBA

ISO

CRACKERS

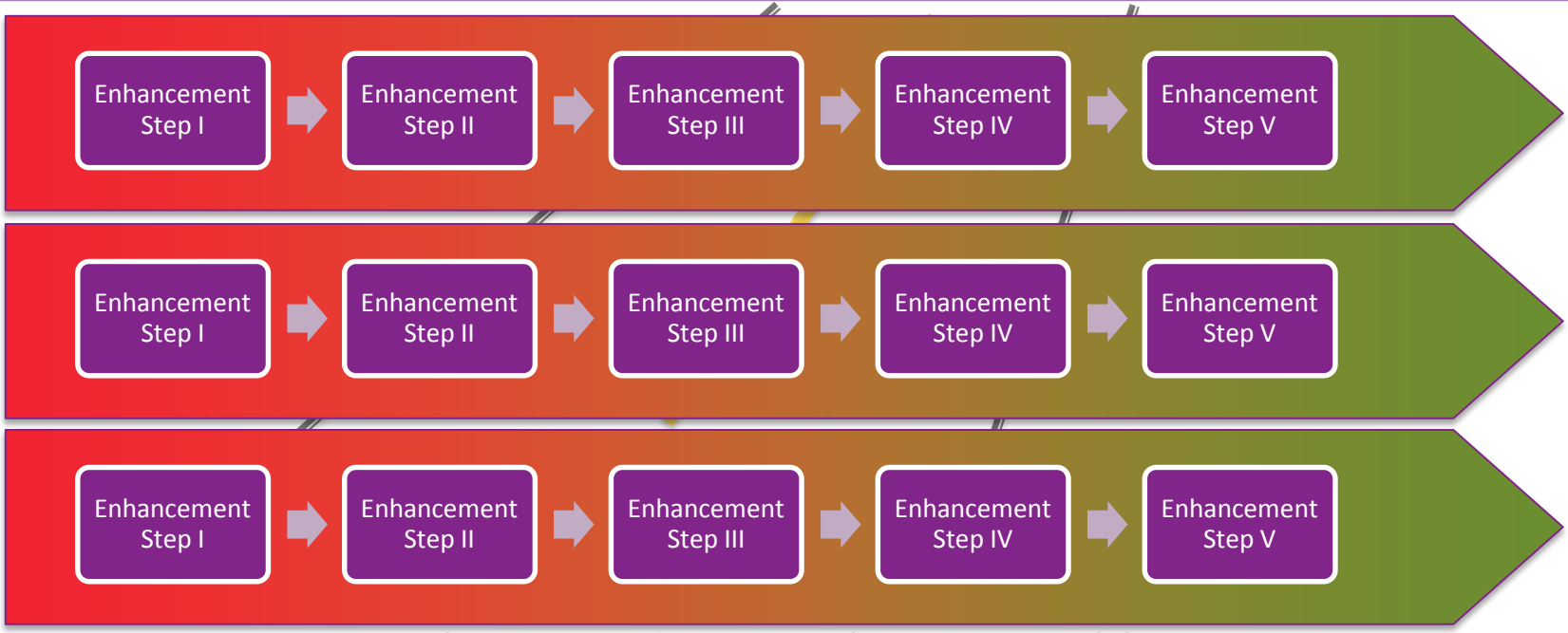
Script Kiddies

NERC

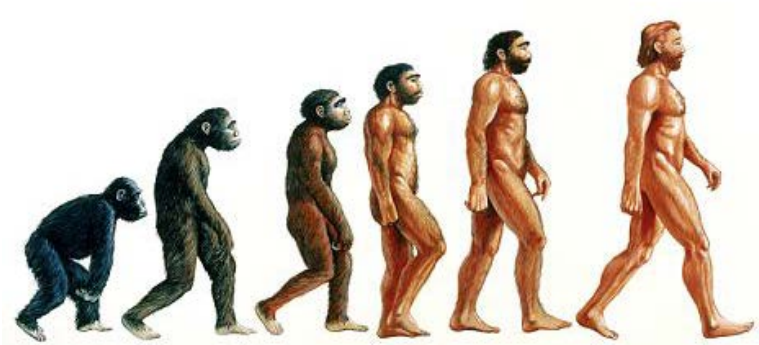
Bruce Bonsall LLC

Formulate a Long-range Strategy …that Fits

Frameworks Add Structure



Lay Out a Realistic Roadmap with Manageable Tactics



Think Evolution, Not Revolution

Launch Your Security Program on an Even Keel

Now Put It Into Action

- Assess the Culture of the Organization
- Build Credibility and Form Alliances
- Clarify Business Challenges with Key Leaders
- Inventory ALL Information Security Assets and Related Resources
- Formulate a Long-range Strategy That Fits the Organization
- Lay Out a Realistic Roadmap with Manageable Tactics
- Launch on an Even Keel

RSA Conference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SEM-M01

Cyber Risk: From the backroom to the boardroom, what *YOU* need to know to survive.

Malcolm Harkins

Global CISO
Cylance, Inc
@protect2enable

#RSAC

Boards by the Numbers

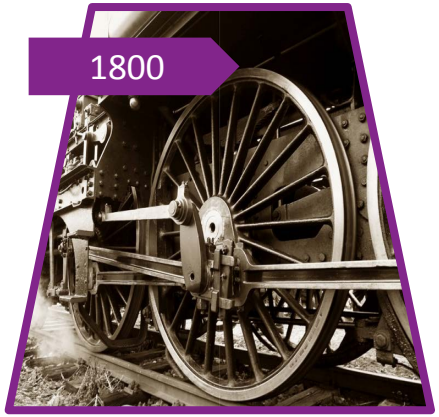
- **75%** of Boards have ***no part*** in reviewing security and privacy risks.
- **32.5%** of Boards ***do not*** receive any infosec information.
- **55%** of Boards ***do not*** receive routine security updates.
- **45%** say even though it is on the agenda ***it is not important***.
- **65%** support punishment such as fines for a data breach.
- **1/6th** of security professionals advocate ***prison sentences*** for CEOs and Board members after breaches!

Information taken from Crime Congress survey March 2015
PWC Global State of Information Security Survey 2015
Boardroom Cyberwatch survey 2014

Questions that Need Answers

- Is Cyber risk accounted for in the corporate planning process?
- What is the process for evaluating security and privacy? And measuring liability?
- Do we have Directors with relevant experience?
- Do we have identified executive ownership?
- What happens in the event of a breach?
- What happens in the event of a vulnerability in the technology we created ?

The March of Technology



Version 1.0

Steam & Coal Power
Railways
Factories
Printing Press
Mass Education

Version 2.0

Electric Lights
Communications
Oil & Gas
Automobiles
Mass Production

Version 3.0

The Internet
Molecular Biology
Renewable Energy
Instant Communications
“Smart” Everything

The World Is Growing More …

COMPLEX

AMBIGUOUS

VOLATILE

The Battle for Control In Cyberspace

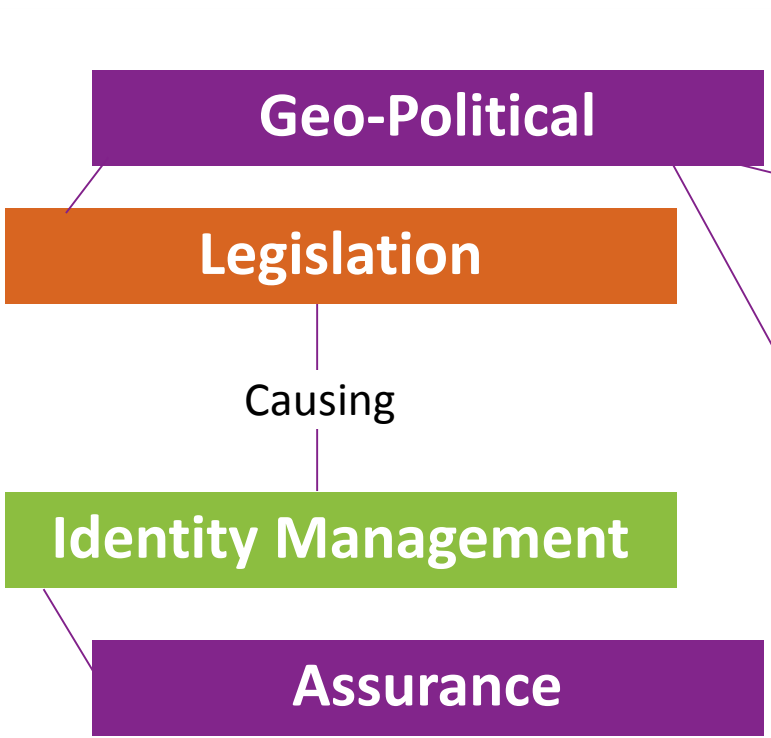
There's a growing debate about the roles of Government and Industry in privacy and security.

Increase in sophistication and number of cyber attacks

Government concerns are driving new regulation

Increasing tensions between privacy and security

A Perfect Storm of Risk

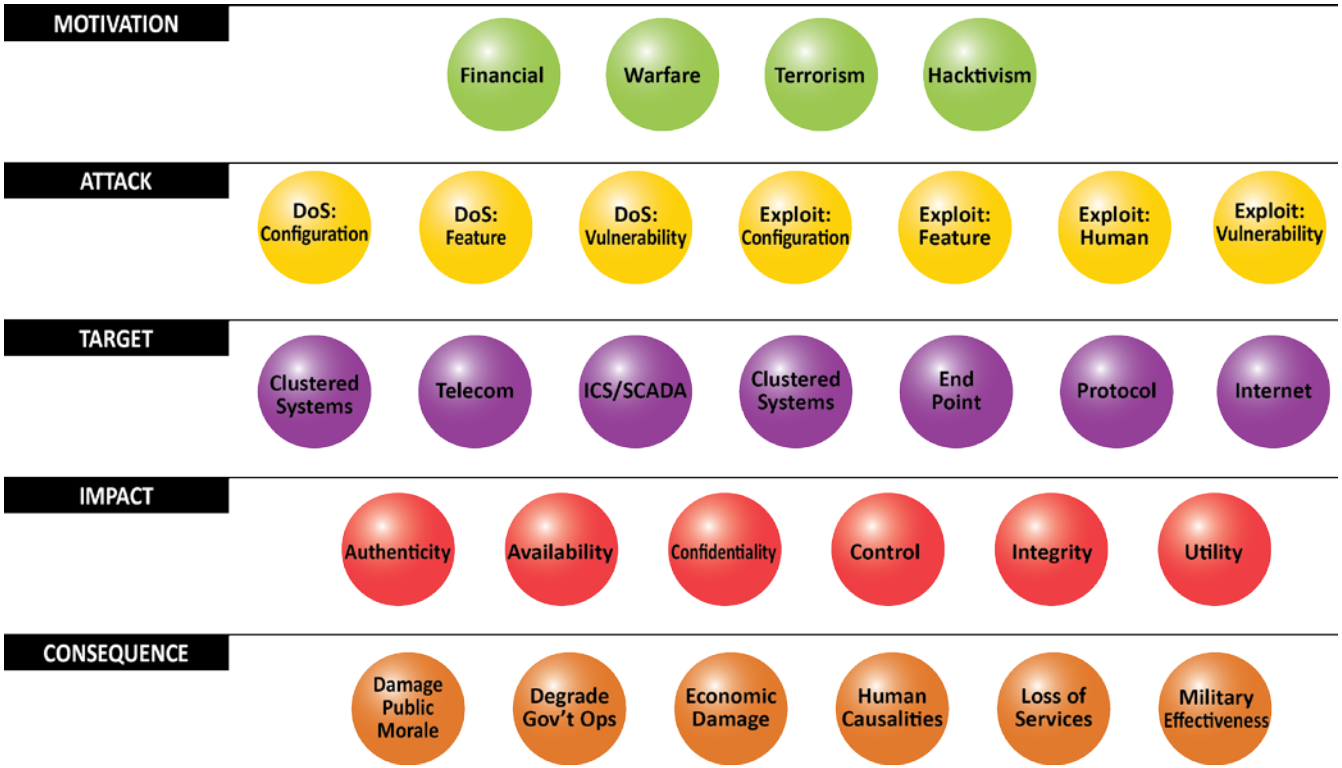


Cyber Threat Landscape

WHY?

WHAT?

HOW?

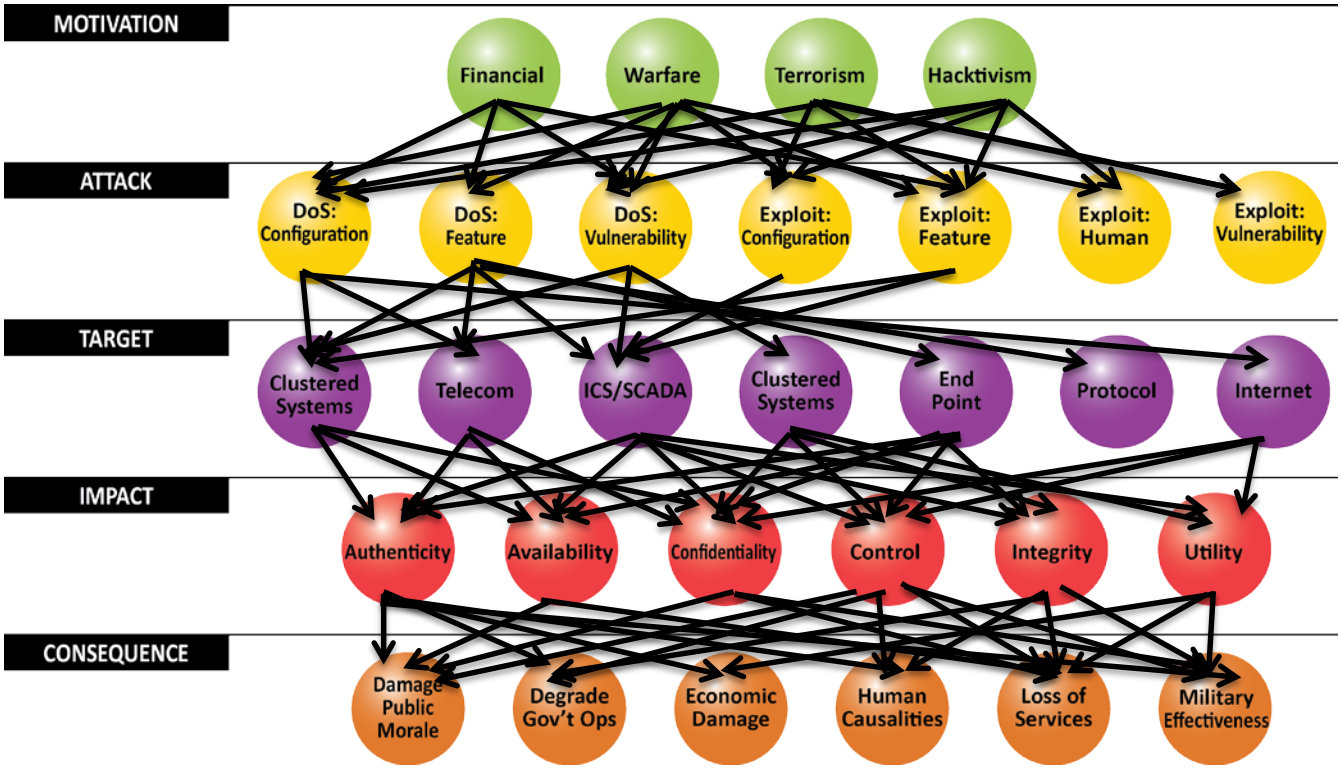


Cyber Threat Landscape

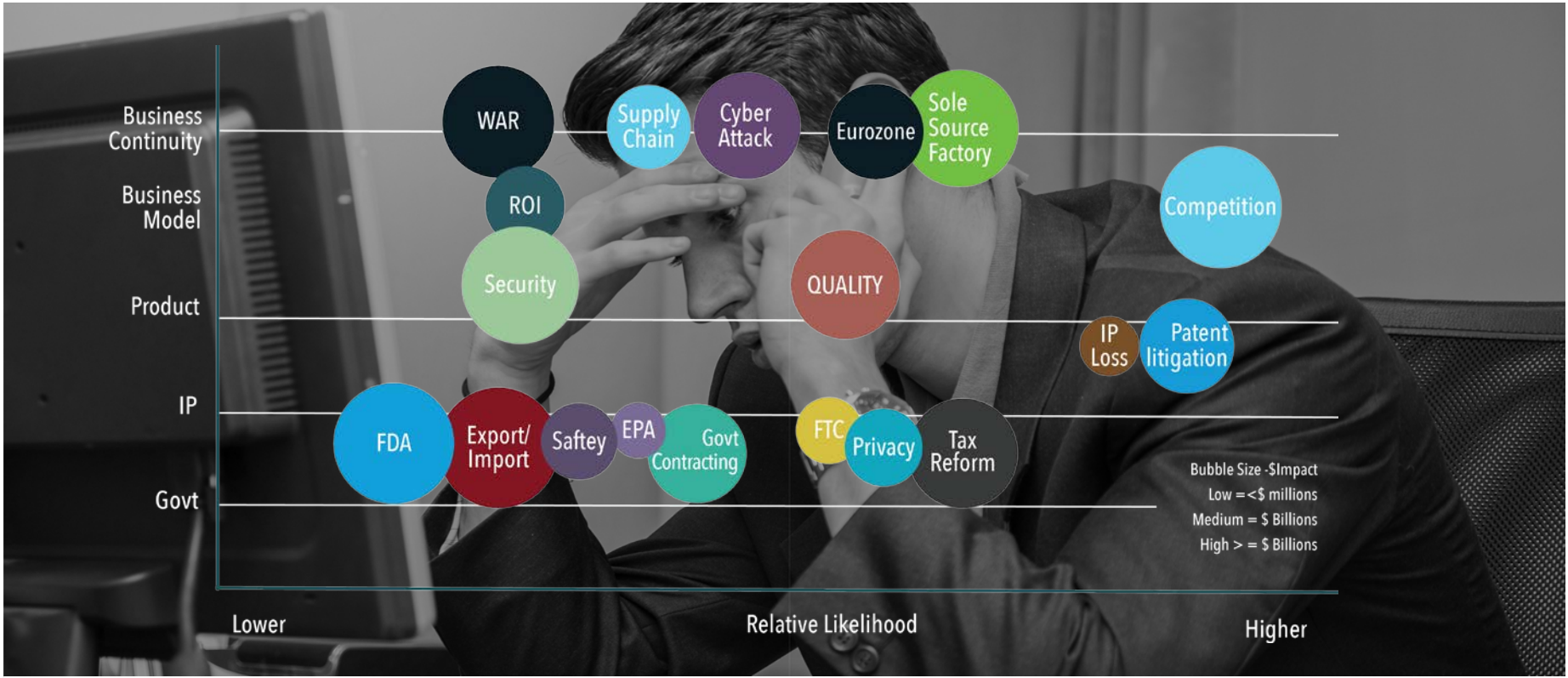
WHY?

WHAT?

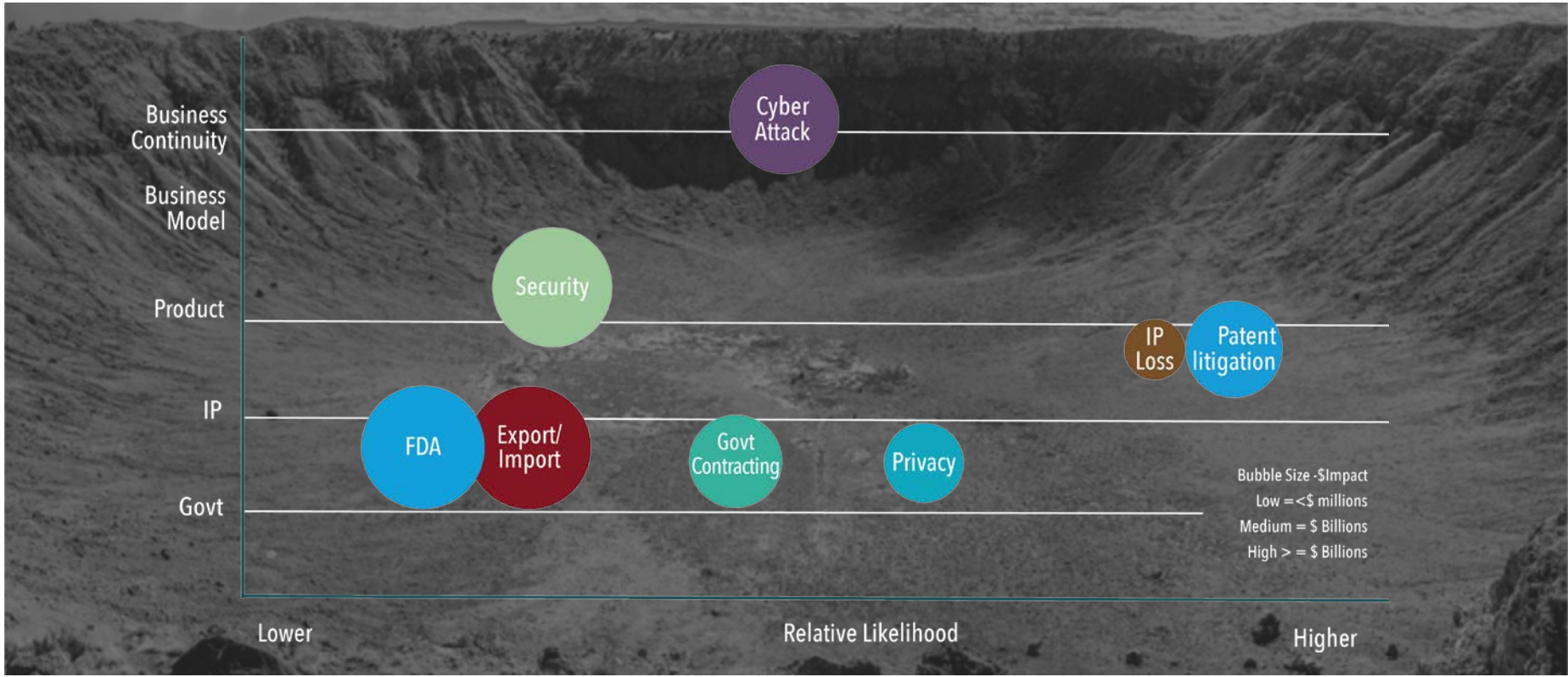
HOW?



What gives the c-suite grey hair?



Privacy & Security Risk IMPACT



Threats & Impacts – A Simple Summary

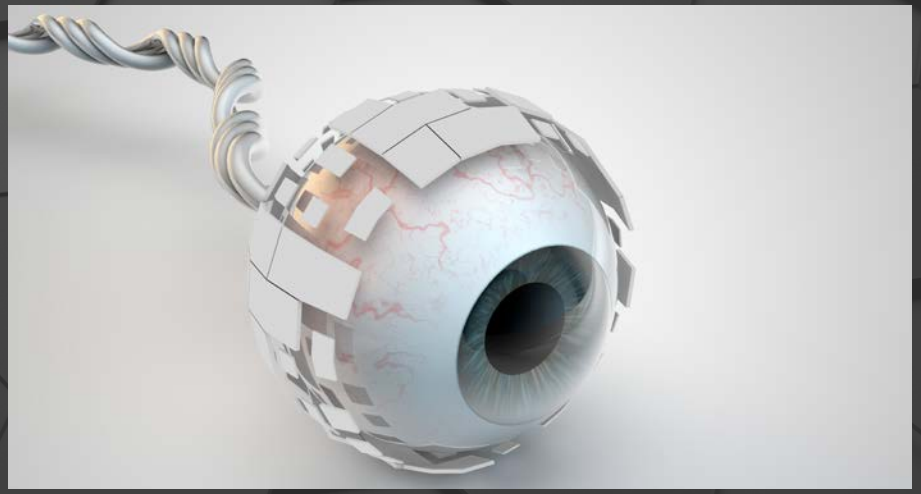
The idea is to assess soil and landscape types, weather and pest issues to boost crop yields and profits.

All the farmer needs is a smartphone, a GPS enabled tractor connected to cloud, with the data & analytics

The idea is to facilitate a precision bombing.

All a government needs is access to the data

The idea is to cure blindness.



Doctors on June 19th 2015 insert a retinal implant into a patients eye that is connected to high tech glasses with a camera and a video processing unit

The idea is to extort money.

All a bad person needs is poorly developed or managed technology and the ability to execute malicious code

The idea is to profit from or to harm others

All a bad person needs is poorly developed or managed technology and the ability to execute malicious code

The idea is to improve food safety and reduce cost

All a food and beverage organization needs is real time information flow from the slaughter house to the point of sale

The idea is to save cows

All a bad person needs is poorly developed or managed technology and the ability to execute malicious code

Digital Evolution

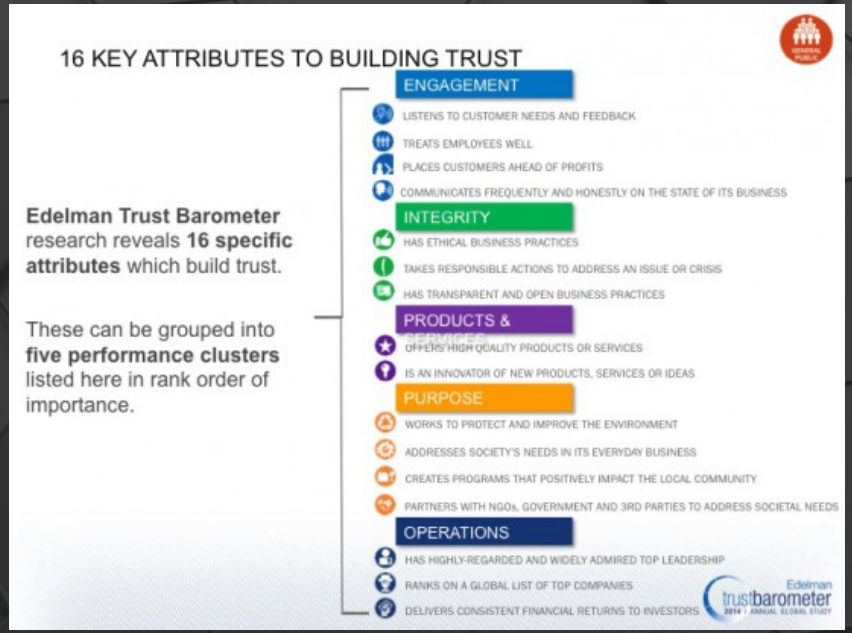
In the next few years the risk landscape will dramatically change:

- Adoption of smart grid devices water/power
- Tech inside more than phones, tablets, laptops
- Proliferation of devices & app markets
- "Virtual assets" - content with emotional attachment in digital world
- IP enabled home appliances
- Centralized home information flow (bundled services via internet)
- Pervasive wearables updating social computing
- Open source Intelligence refining targets

Expanding attack surface - greater technology integration with society well being

Cyber ~~has been~~ IS ~~characterized as~~ the 5th domain of warfare

A growing digital economy relies on Trust Evolution



"We saw air let out of the balloon, an evaporation of trust"

"the reputation of the Tech industry went backwards"

"By a margin of 2 to 1 people don't believe that governments or businesses are thinking enough about the broad negative societal impacts that technology can have"

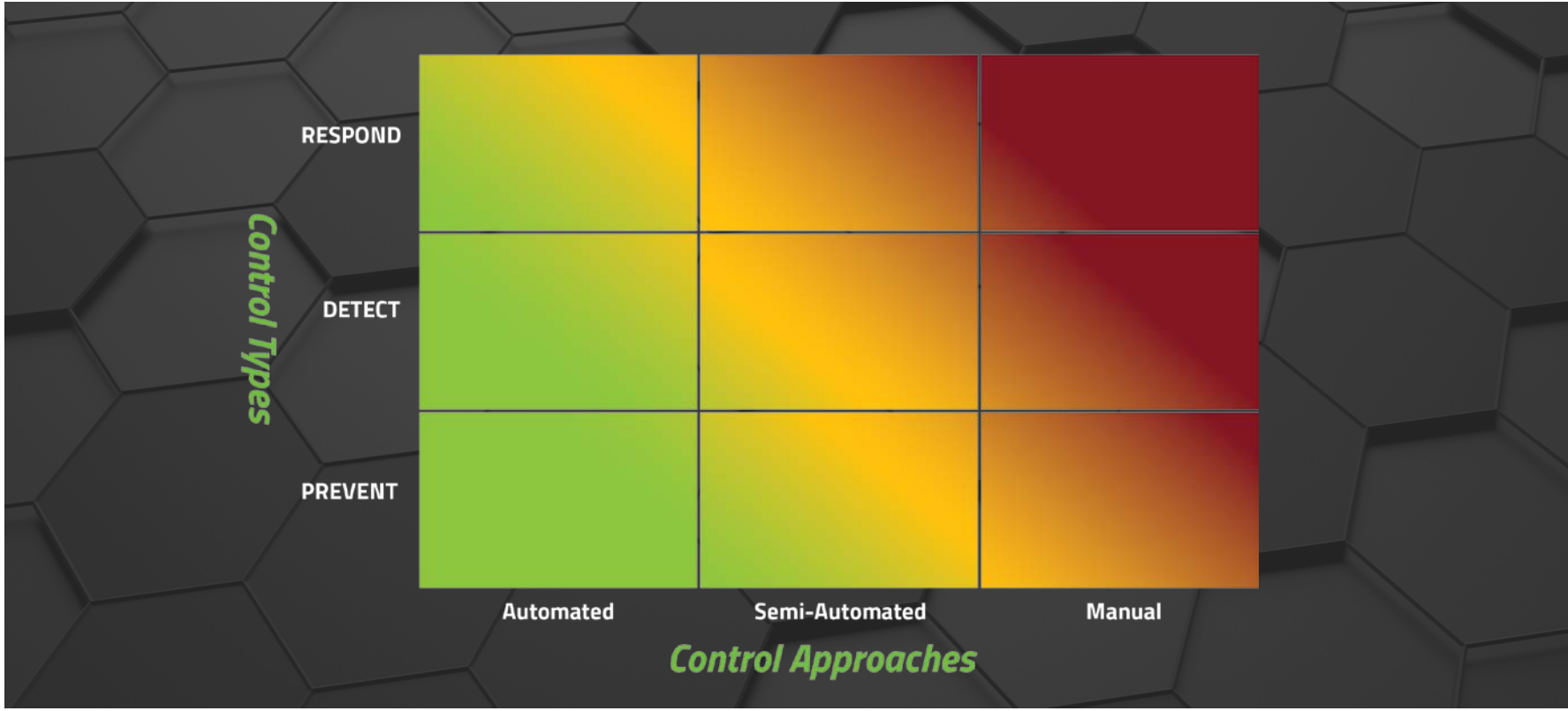
Richard Edleman – Feb 2015

Breaking someone's trust is like crumpling up a perfect piece of paper

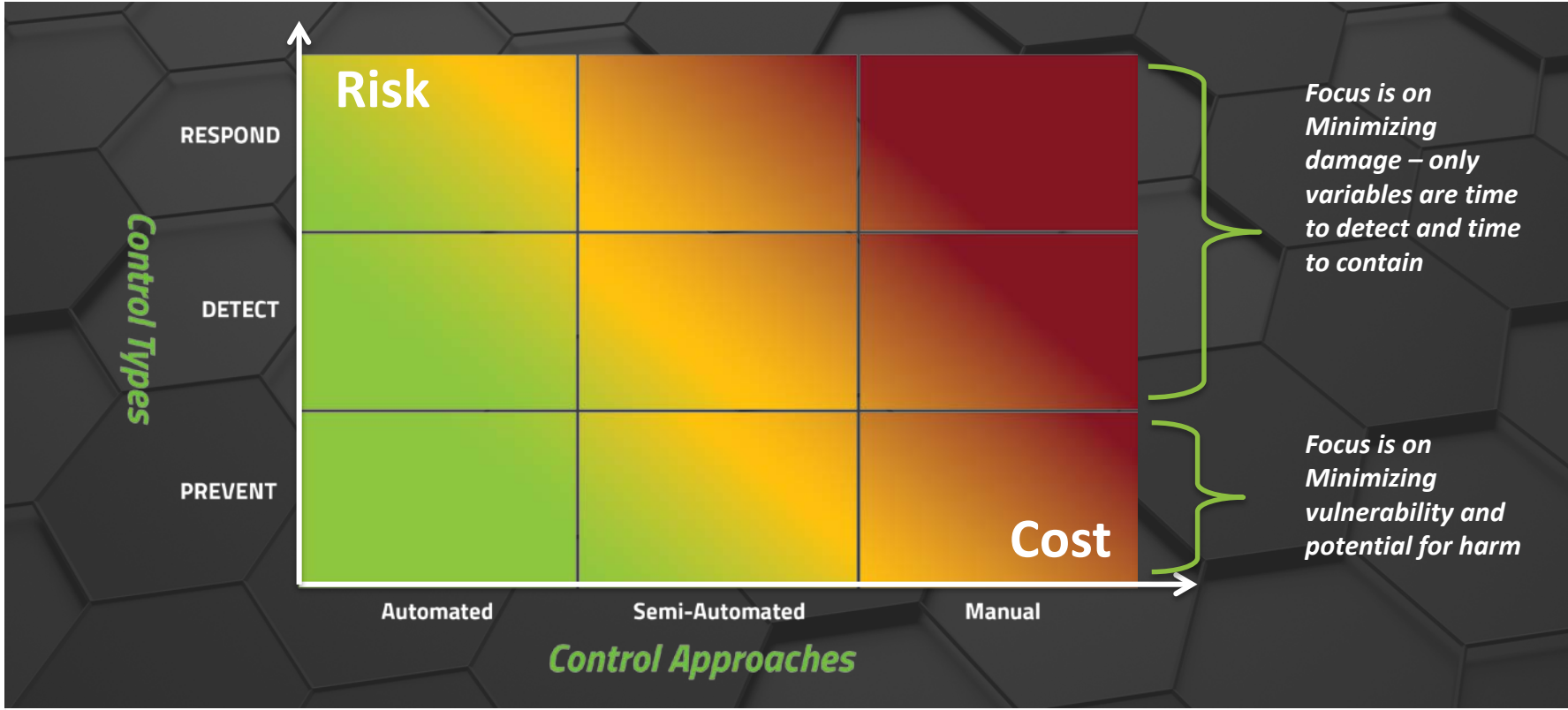
Breaking someone's trust is like crumpling up a perfect piece of paper

You can work to smooth it over, but it's never going to be the same again

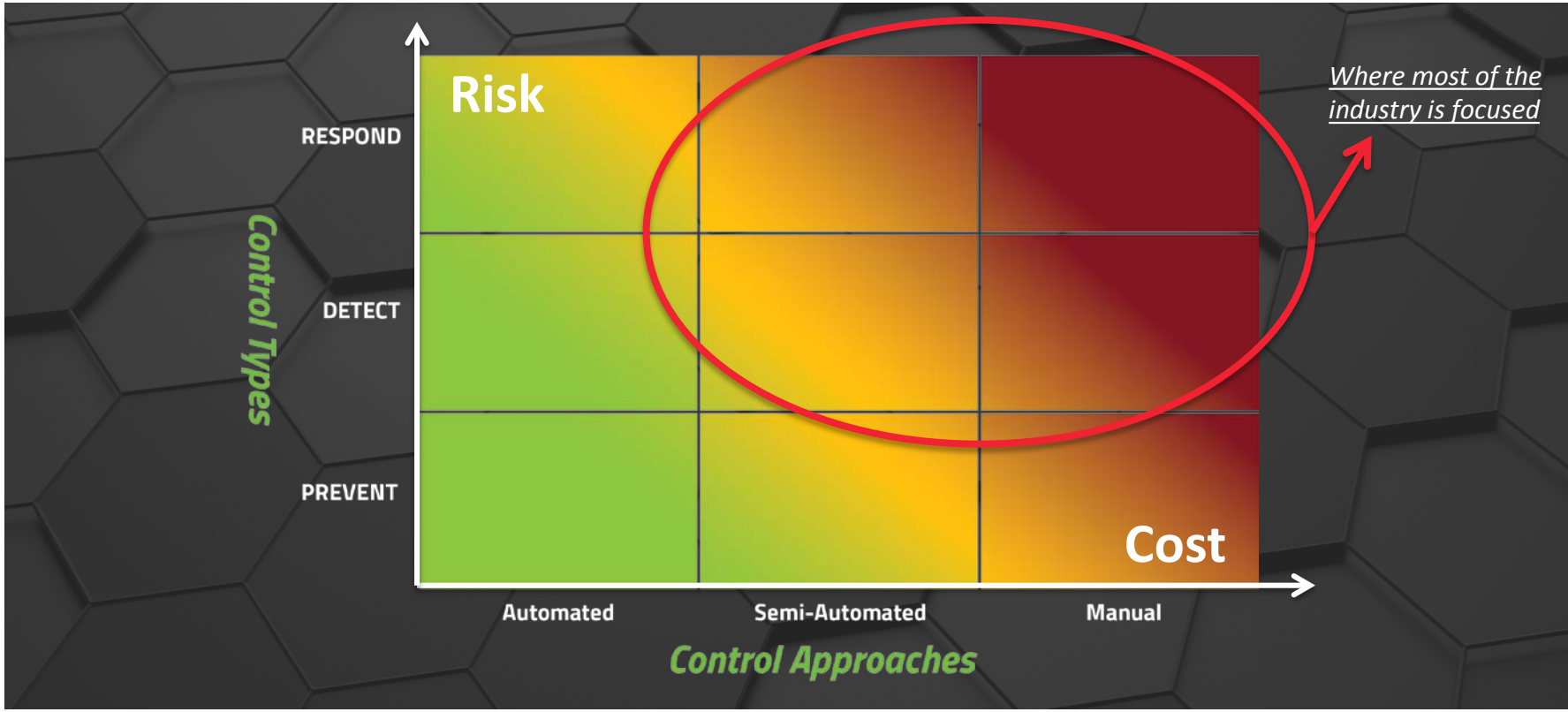
9–Box of Controls



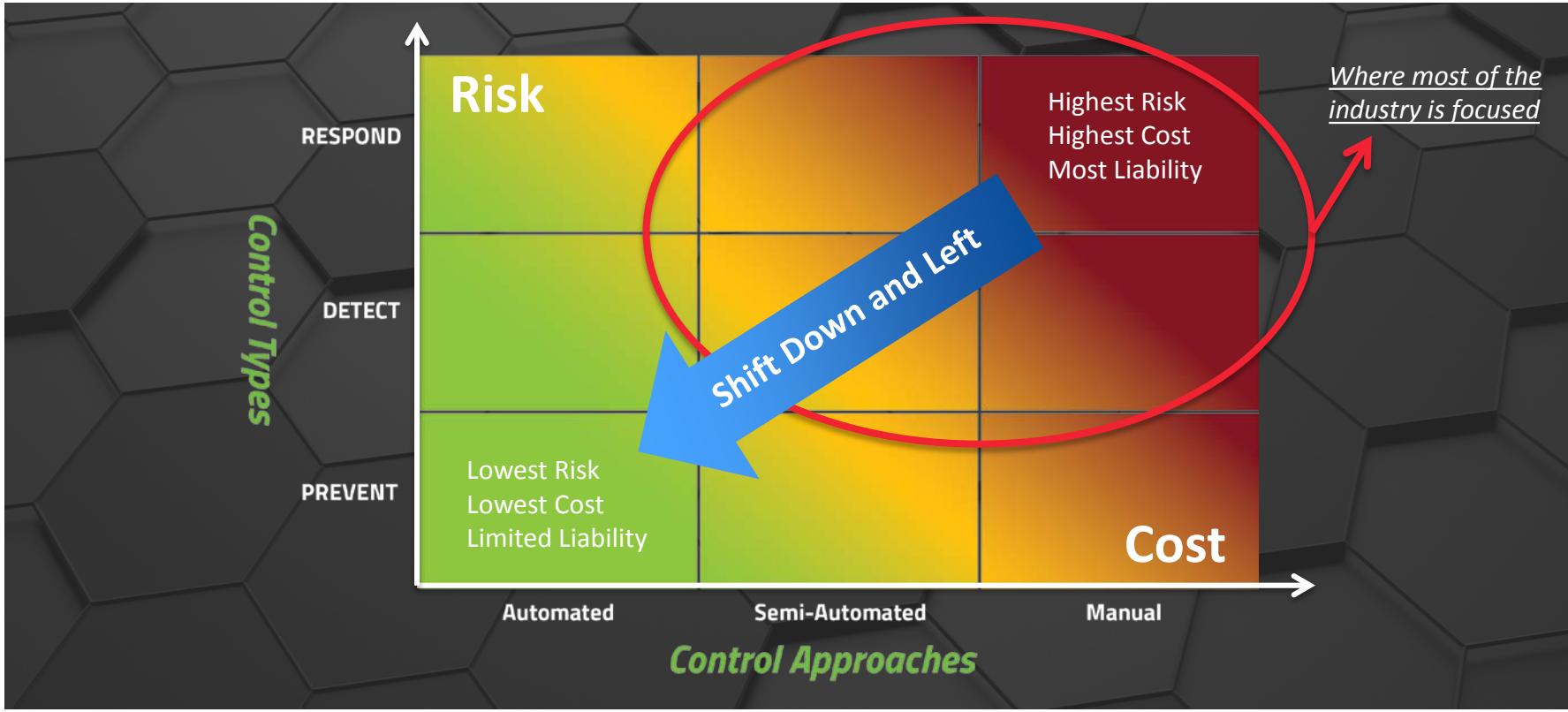
9–Box of Controls



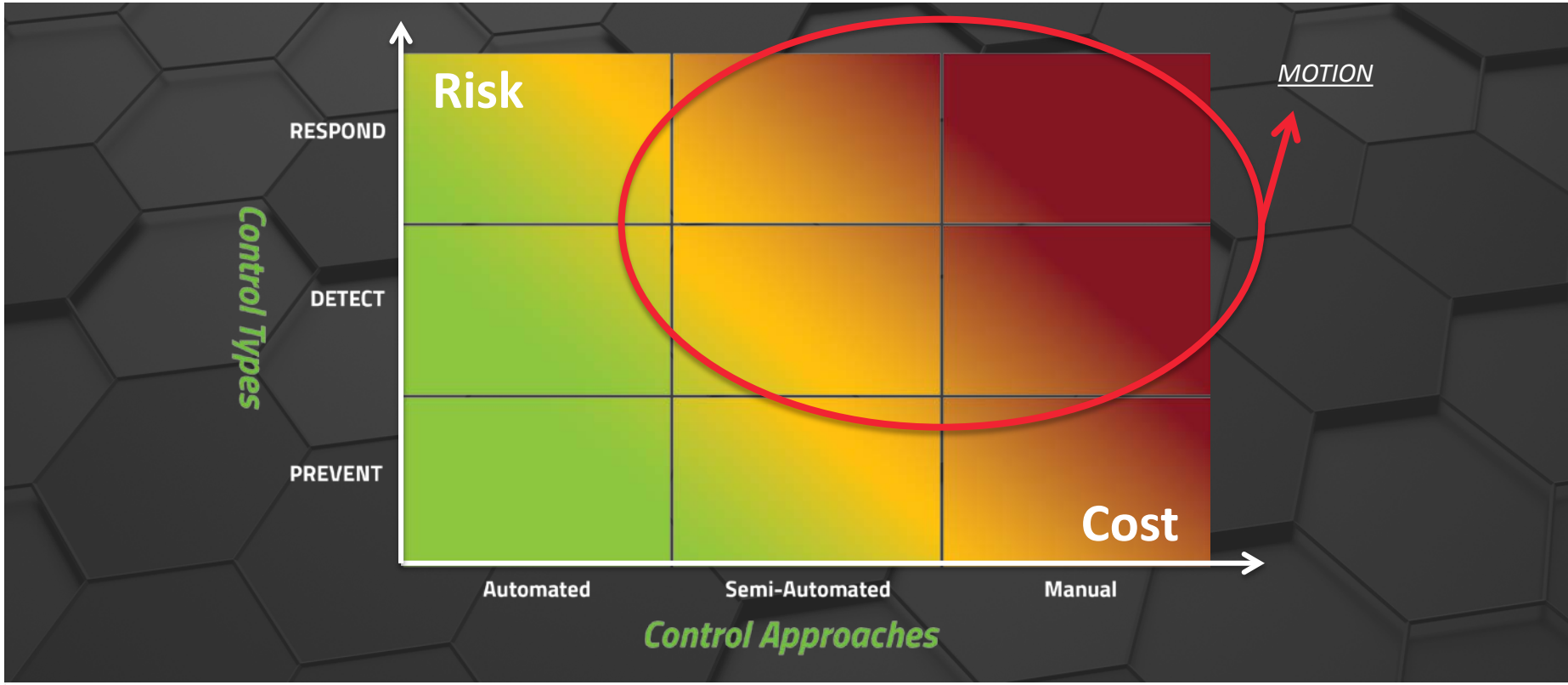
9–Box of Controls



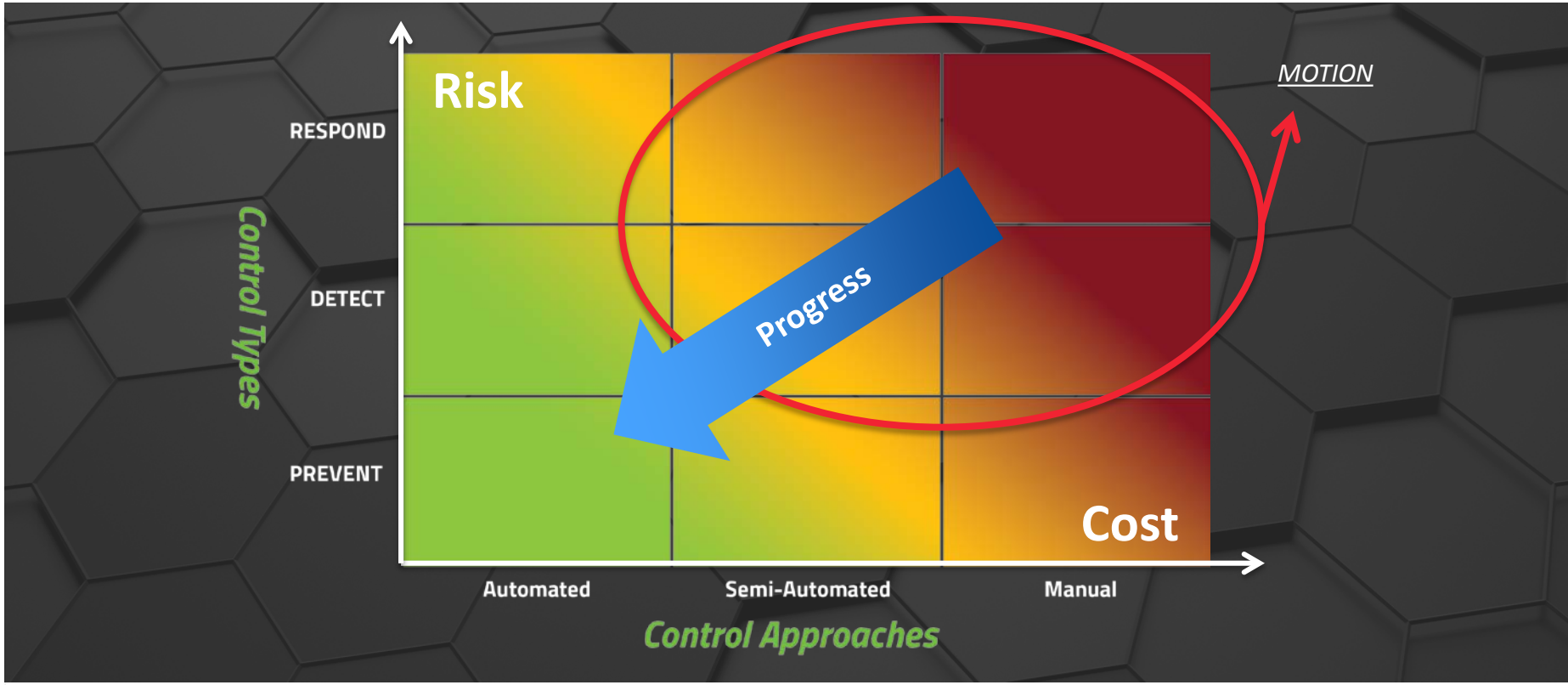
9–Box of Controls



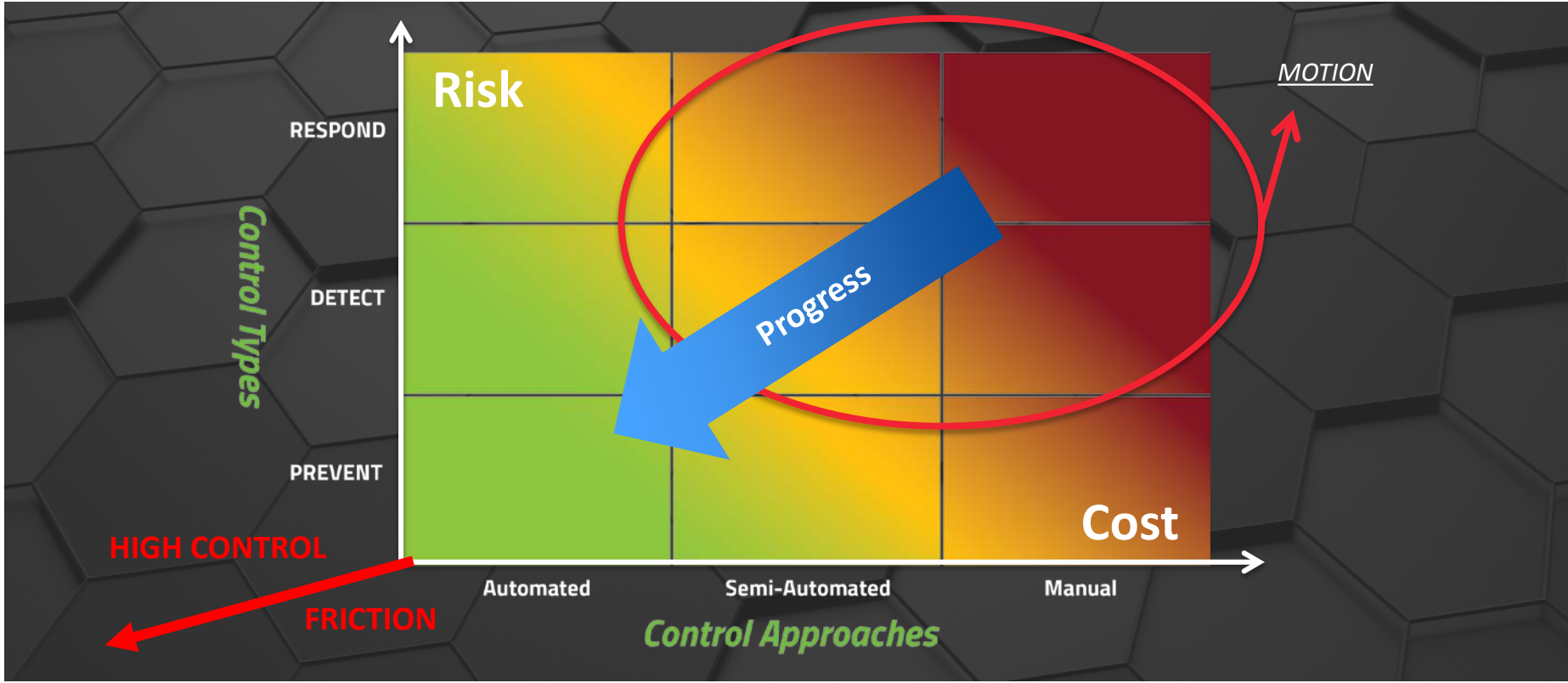
9–Box of Controls



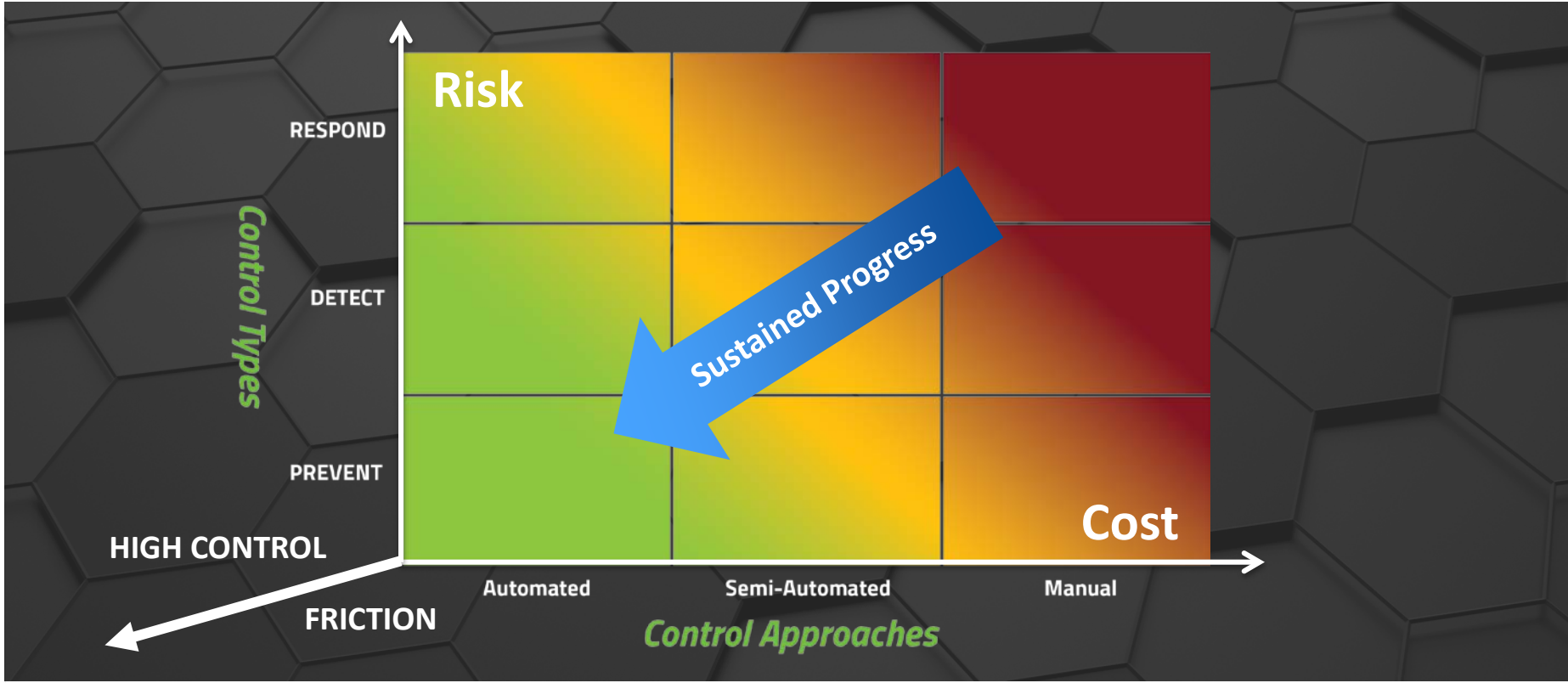
9–Box of Controls



9–Box of Controls

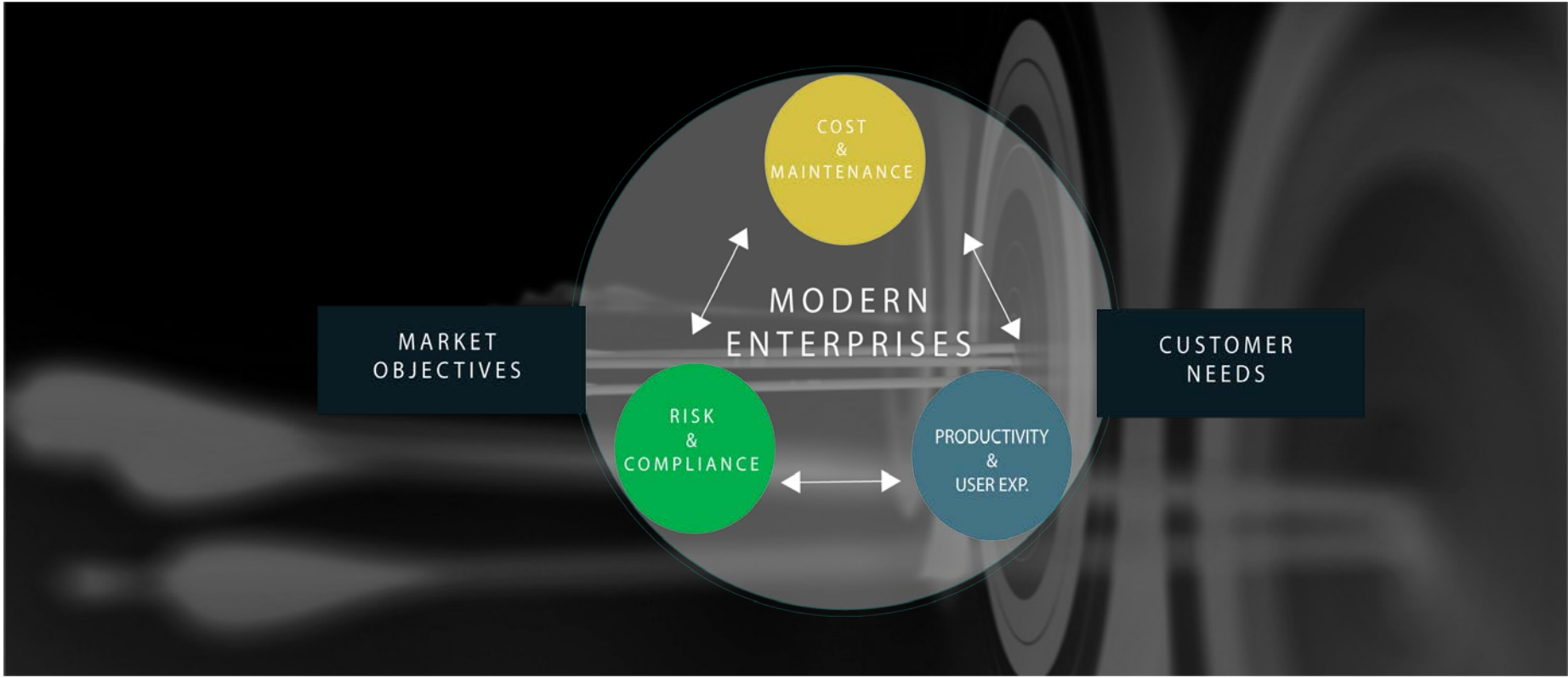


9–Box of Controls



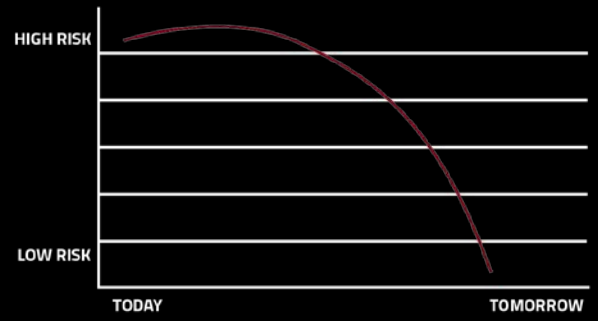

IT'S ALL ABOUT
PROTECTING TO ENABLE
PEOPLE, DATA, AND
BUSINESS.

Need to be Tuned to Target

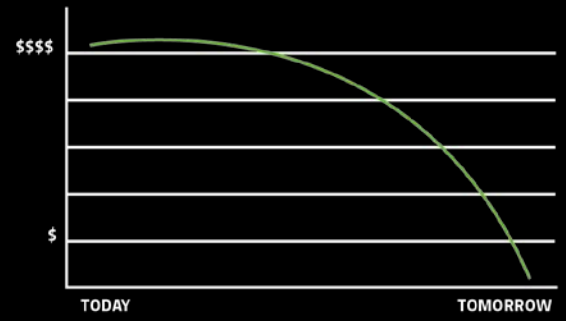


We Need Solutions that…

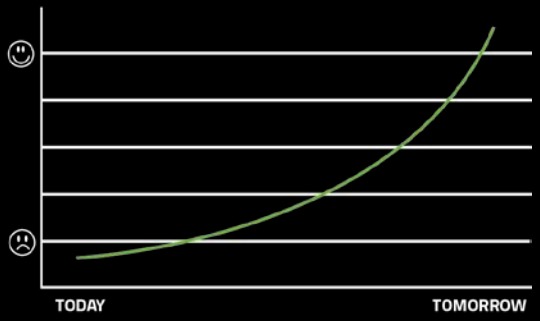
LOWER RISK



LOWER COST



LOWER FRICTION



To Enhance Trust in Technology

Board Discussion Coaching Tips

Learn What Works	Explore with others who have presented	Careful to not use 'security geek speak'	Seek out stakeholders for input and potential pre-review (Marketing, IT,Legal, Mfg., Corp Affairs, Public Policy, Business GM's
Know Your Audience	Who are your Board Members?	Discover their background	Know what you want them to walk away knowing or understanding

Know Your Role

What to Present

- Determine scope (wide angle view) then re-scope to the critical few hot or emerging topic areas Internal operations, external facing systems, products/services, IP protection, privacy, availability risks…
- Make the connection to your Enterprise Risk Map and the 10 Universal Business Risks
- Share notable events, issues, excursions & lessons learned
- Highlight you will never be incident free & give confidence of your ability to handle
- Don’t ask for money – generally not the Board’s role
- Provide data & indicators and have back up with more data
- Budget time, material, Q&A and discussions

Presenting Your Information

- Understand your business and key drivers of the business model – how does it connect with cyber & privacy risks
- Distill complex topics, don't hide the complexity, show you understand and simplify (recent & newsworthy cyber/privacy items)
- Never read the slides…tell the story and use material as your props
- Practice…Practice…Practice – avoid surprise questions
- Have an executive summary & consider a 3-5 page white paper sent a couple weeks beforehand

Closing Thoughts

Understand: Who you work for vs. Who you report to

- Don't get confused on them
- Accept coaching on managing the message but not massaging the message

Characterize: Consequence & Impact

- To the organization
- To the shareholders
- To the customers
- To Society

Own: Your Accountability

- For asking the "high contrast" questions to expose the contours of risk
- For delivering the message that needs to be heard
- For the result – Both the impact of risks & the controls

RSA Conference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID:

The Long Walk to the CEO's Office

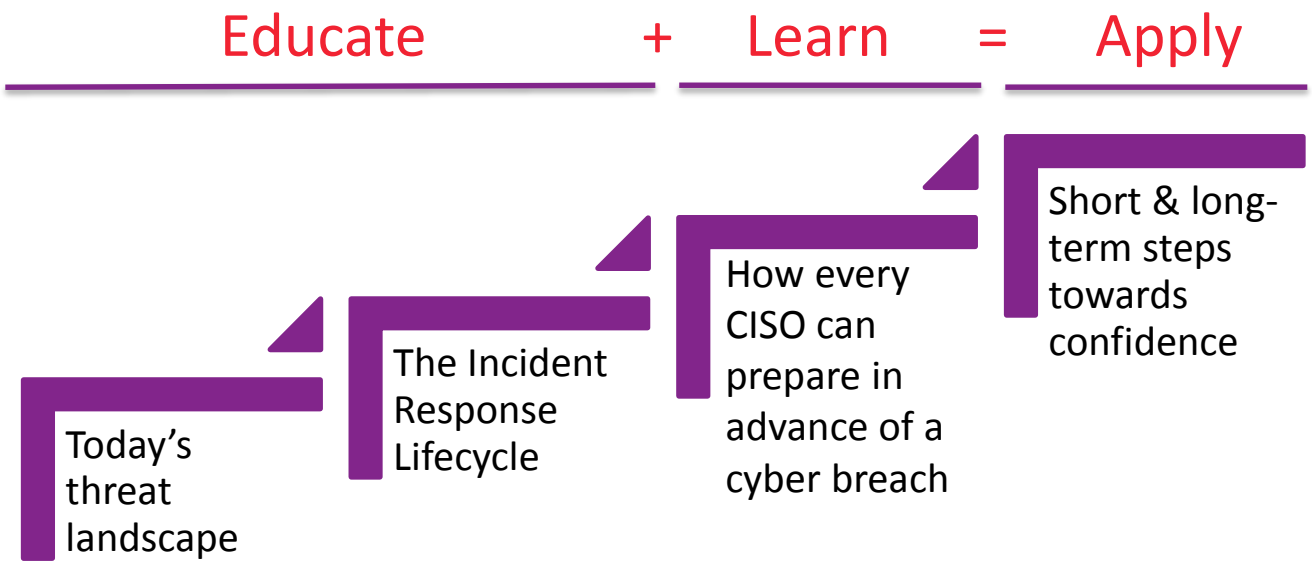
JB Rambaud

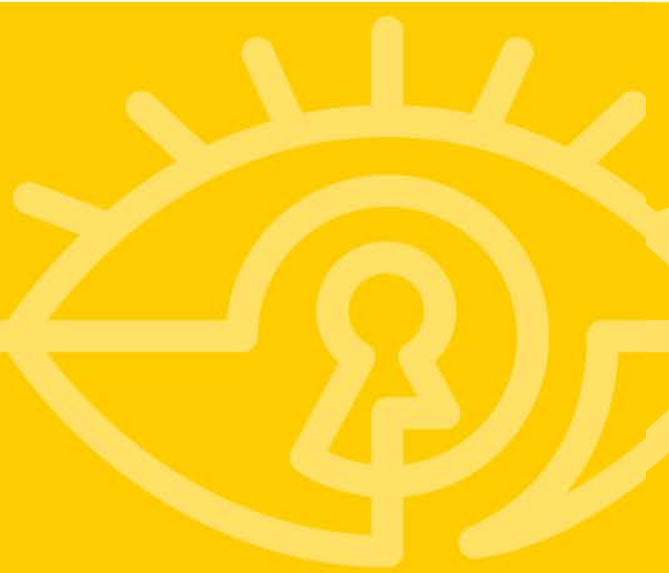
Managing Director
Stroz Friedberg
JRambaud@strozfriedberg.com

#RSAC


Our Disaster Recovery Plan Goes Something Like This...
HELP!
HELP!
DILBERT
By Scott Adams

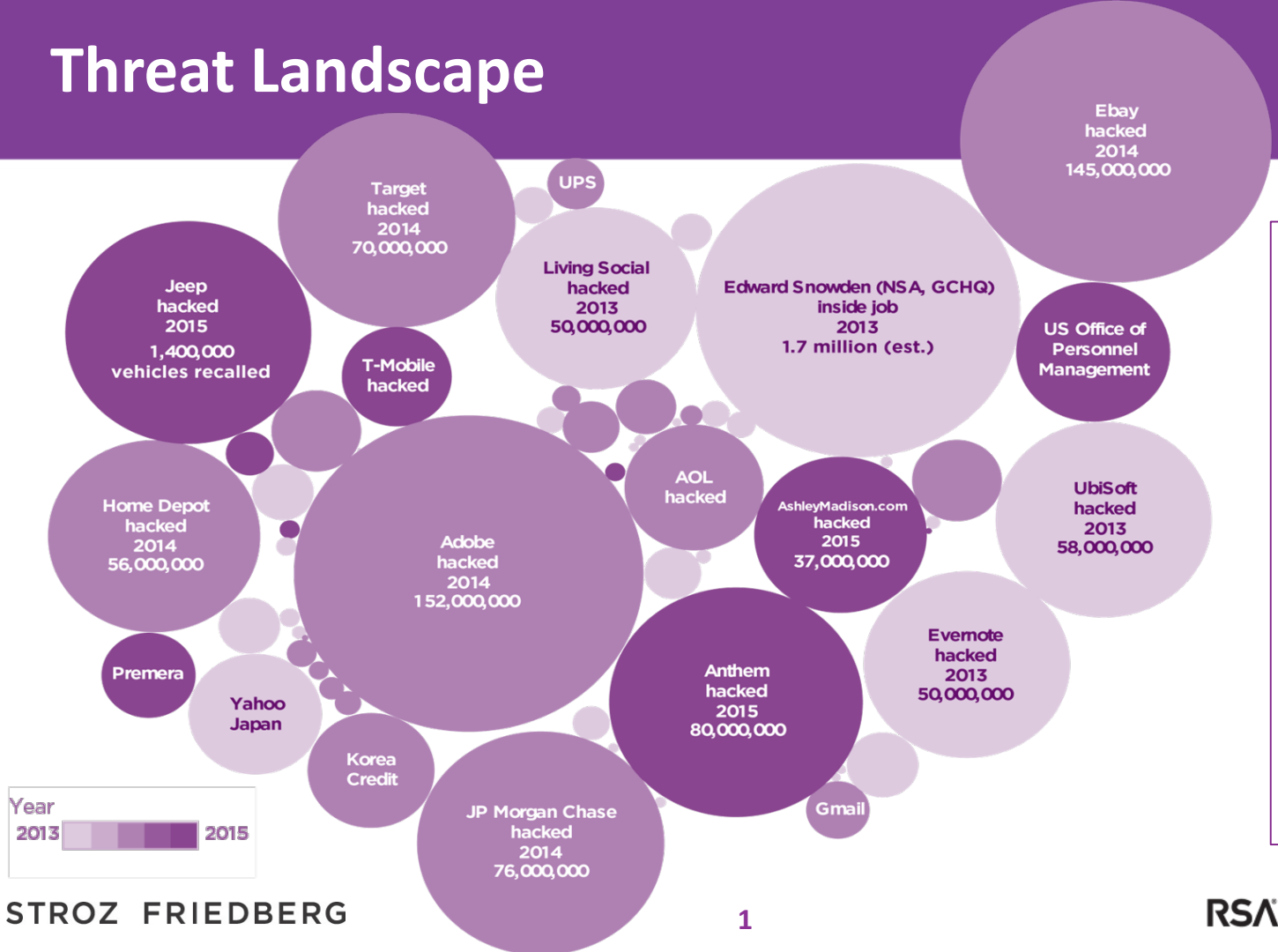
How to Gain Confidence in Your Program





Today's Threat Landscape

Threat Landscape



The Biggest Security Threats in 2016[1]

- Extortion Hacks
- Attacks that Change or Manipulate Data
- Chip-and-Pin Innovation
- The Rise of the IoT Zombie Botnet
- More Backdoors

[1] *Wired Magazine,* January 1, 2016.

Why Is It Harder Today to Protect Ourselves?

Shareholder Value

Brand & Reputation

Corporate Data

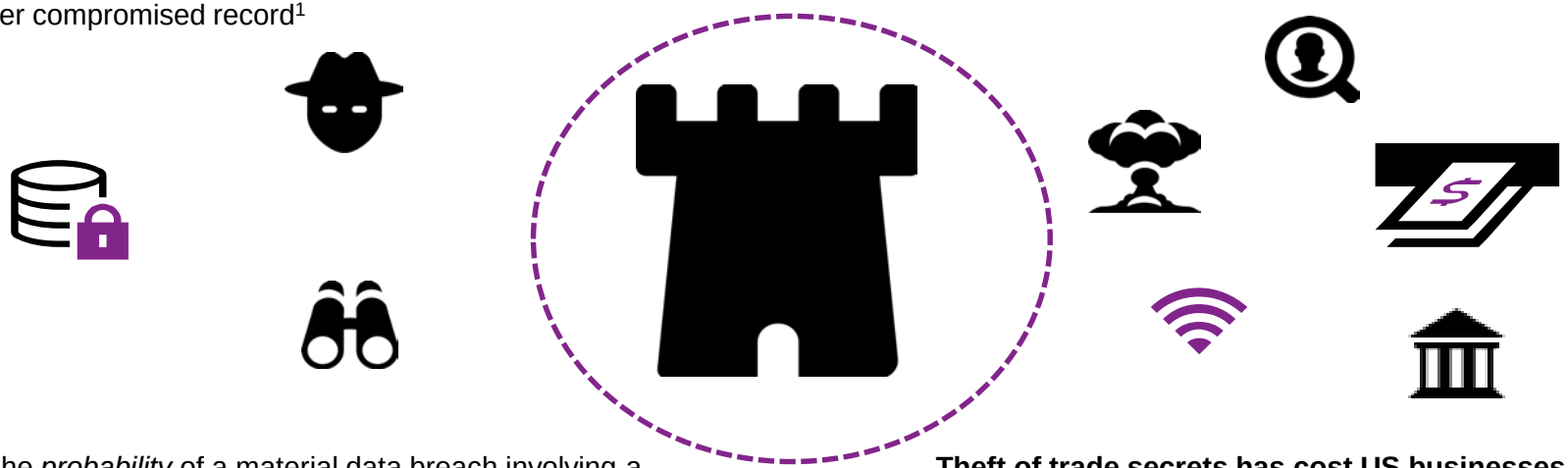
People's Lives & Well Being

Privacy of Information & Communications

What Are We Protecting?

US companies experience the **most expensive data breach incidents** caused by malicious or criminal attackers at $246 per compromised record[1]

32% say **insider crimes are more damaging and costly** than those perpetuated by outsiders[2]

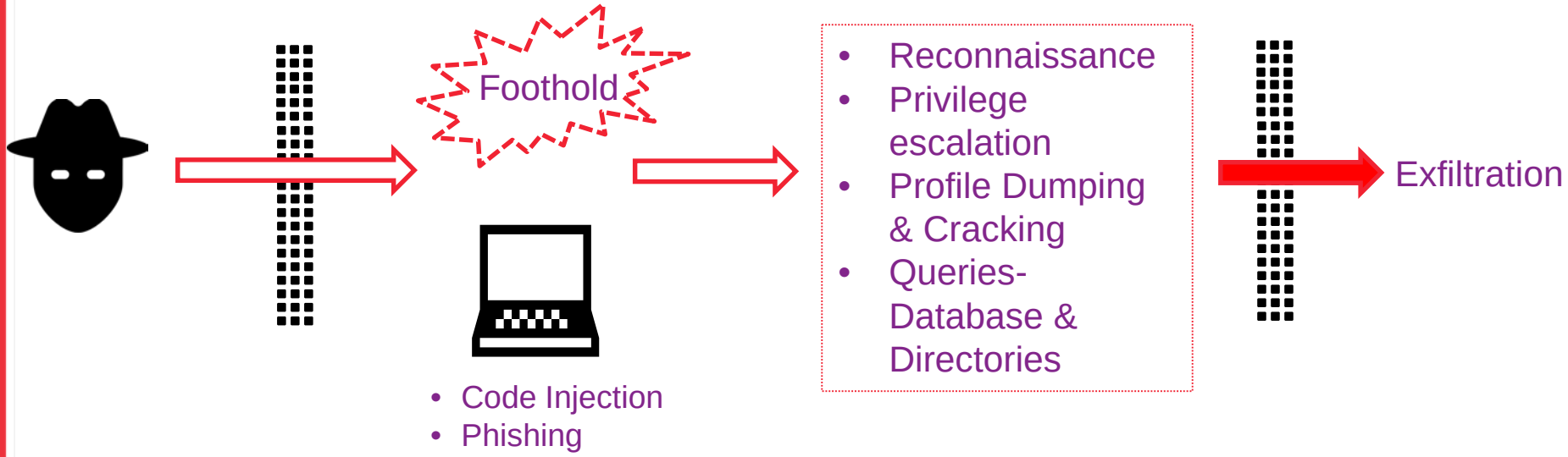


The *probability* of a material data breach involving a minimum of 10,000 records is **more than 22 percent**[3]

Theft of trade secrets has cost US businesses $250 billion per year and are expected to double in the next decade[4]

[1] "Global Cost of Data Breach Increased by 15 percent", Ponemon Institute, May 5, 2014.
[2] "2014 US State of Cybercrime Survey", co-sponsored by *CSO Magazine*, CERT Division of the Software Engineering Institute at Carnegie Mellon University, PwC, and the US Secret Service.
[3] "2014 Cost of Data Breach Study: Global Analysis", Ponemon Institute.
[4] Vormetric's 2015 Insider Threat Report.

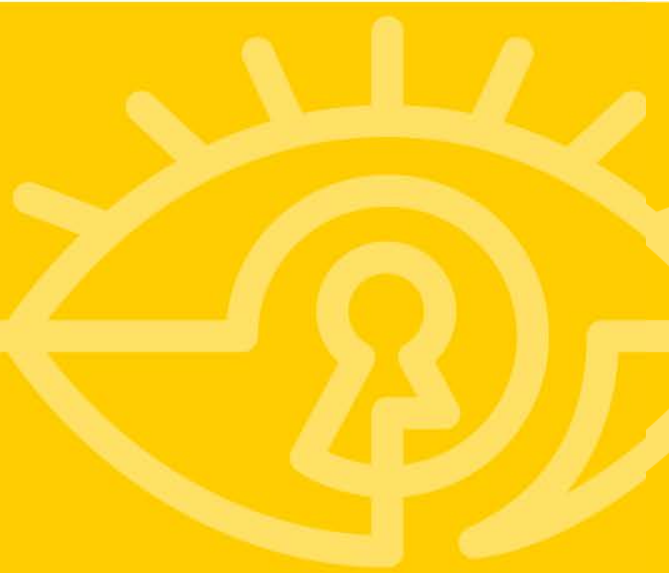
Anatomy of an Advanced Attack



Intrusion Defense

- White Listing
- Anomaly Detection
  - Automated
  - Log Monitoring & Exchange
- Dual factor on Domain Accounts/Privilege Account
- Temporary Admin Accounts
- Strong Passwords
- Data Hygiene
- Ethical Hacking (Simulate Advanced Attack – Blue and Red Teaming)

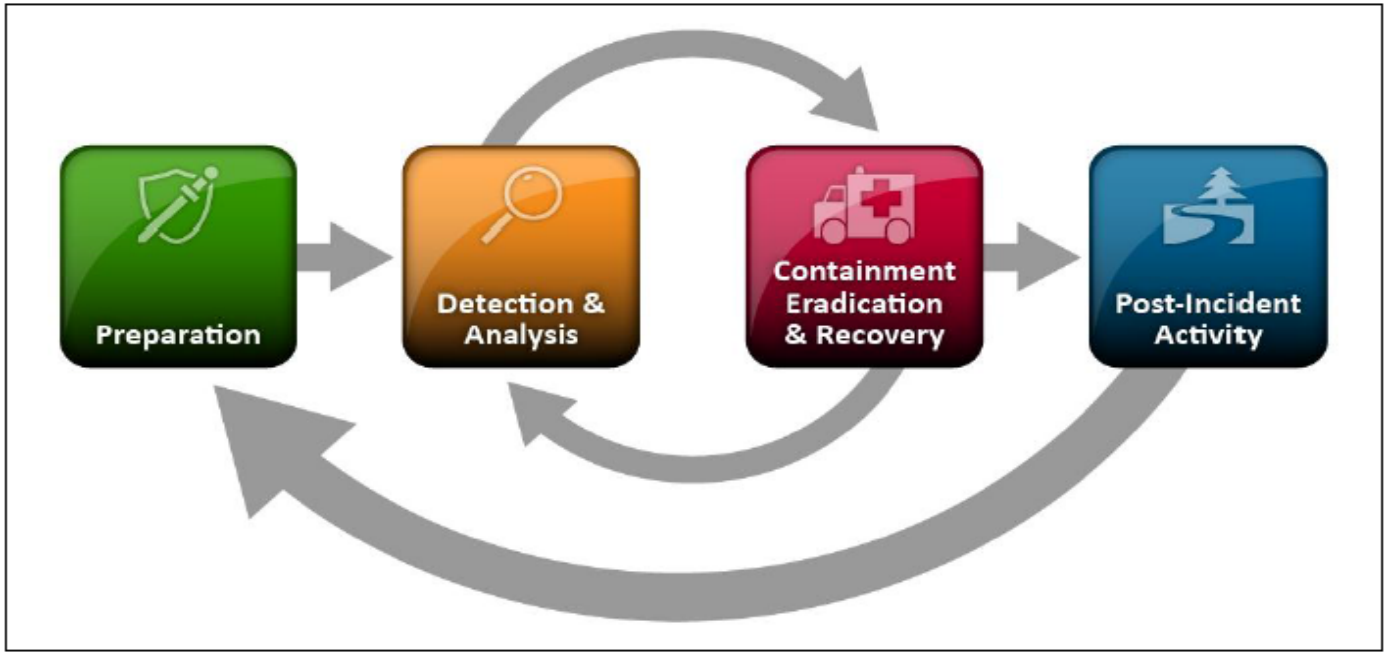
Insider Risk Detection and Prevention



The Incident Response Lifecycle

Cyber Resilience = A Process
(Not a Destination!)

Incident Response Lifecycle



Source: "Computer Security Incident Handling Guide," NIST Special Publication 800-61, rev 2 (2012)

Breach Preparation

Conducting a Risk Assessment

- Select an appropriate security standard
  - (NIST, HIPAA, ISO, PCI, Safeguards Rule, etc.)
- Comprehensive Risk Assessment via interviews and automated tools
- Analyze vulnerabilities relative to current threat intelligence
- Develop risk scenarios based on likely attack vectors
- Provide prioritized recommendation's on risk mitigation
- Integrate all key findings into governance program/metrics to track strategic progress

Breach Detection & Analysis

Investigate, Monitor & Contain

- **Triage**, **Engage** and **Initiate** investigation and containment
- **Categorize**, **Monitor** and **Analyze** incident level by type and severity
- **Activate** appropriate IR handling procedure based on the Incident

Breach Recovery

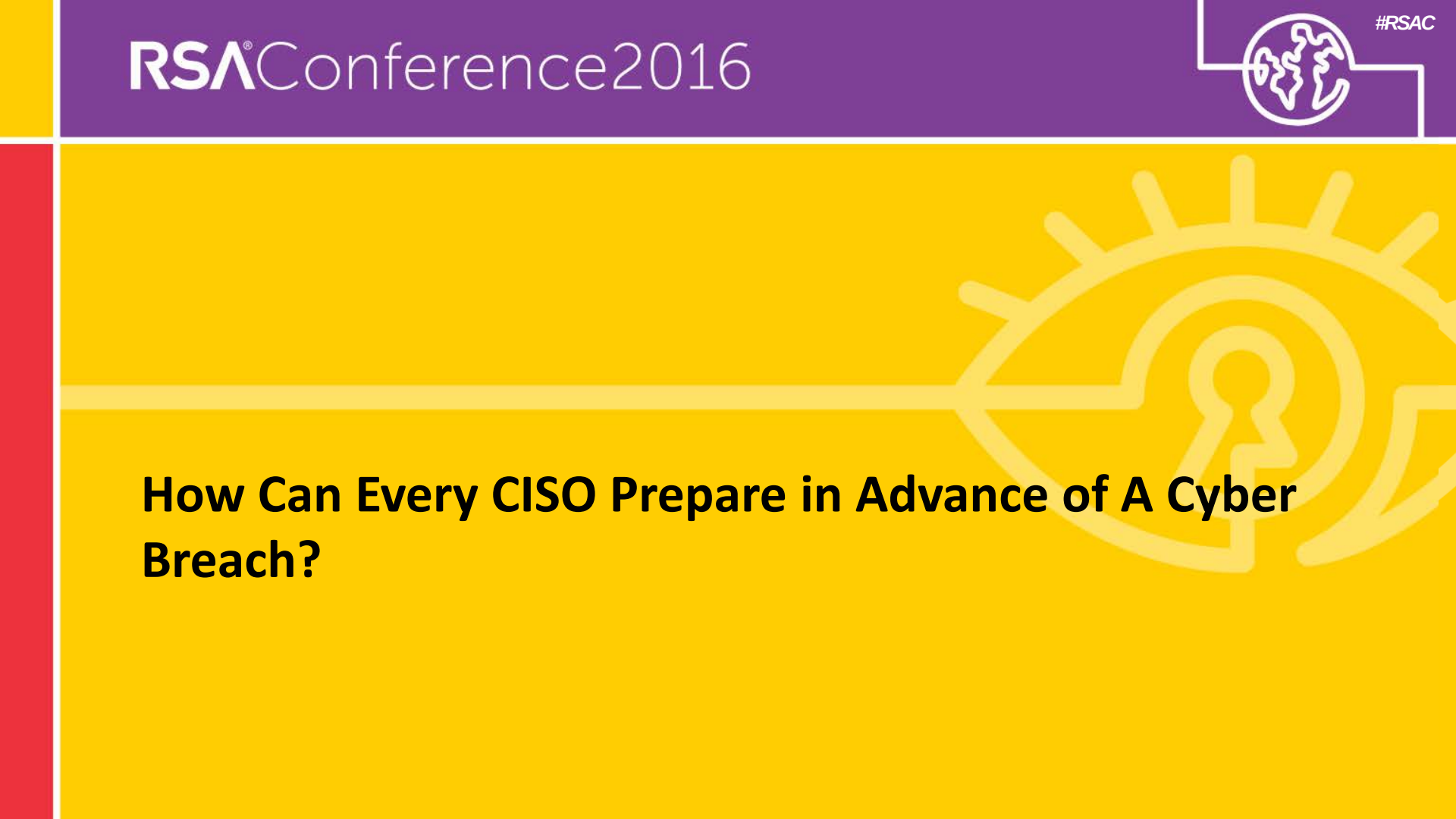
Complete Investigation, Impact Analysis, and Corrective Action Plan

- Determine full scope of incident
- Develop recovery plan
- Document impact assessment and corrective actions
- Restore normal operations
- Develop detail recovery plan procedures

Post-Incident Activity

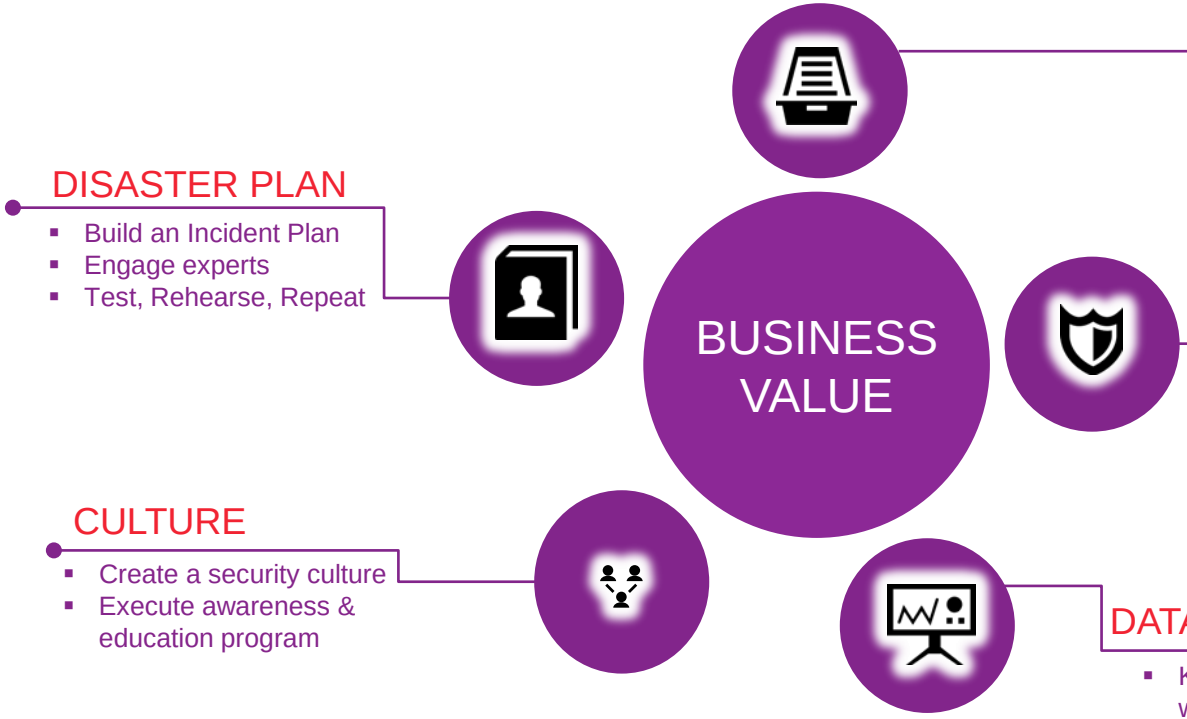
Post-Incident Analysis

- Remediate any remaining technical or process controls
- Pursue Financial and Regulatory/Litigation Recovery
- Develop guidelines on recovery procedures
- Perform lessons learned exercise
- Review and make improvement to the Response Plan and Security Program
- Update Response plan metrics



How Can Every CISO Prepare in Advance of A Cyber Breach?

Preparation



GOVERNANCE

- Govern cyber resilience: determine “if” and “how” security objectives are achieved
- Gather stakeholders and build team – internal & external partners
- Elevate reporting to CEO/Board
- Allocate appropriate budget

DISASTER PLAN

- Build an Incident Plan
- Engage experts
- Test, Rehearse, Repeat

THREAT PROFILE

- Know your profile
- Consider inside & outside threats

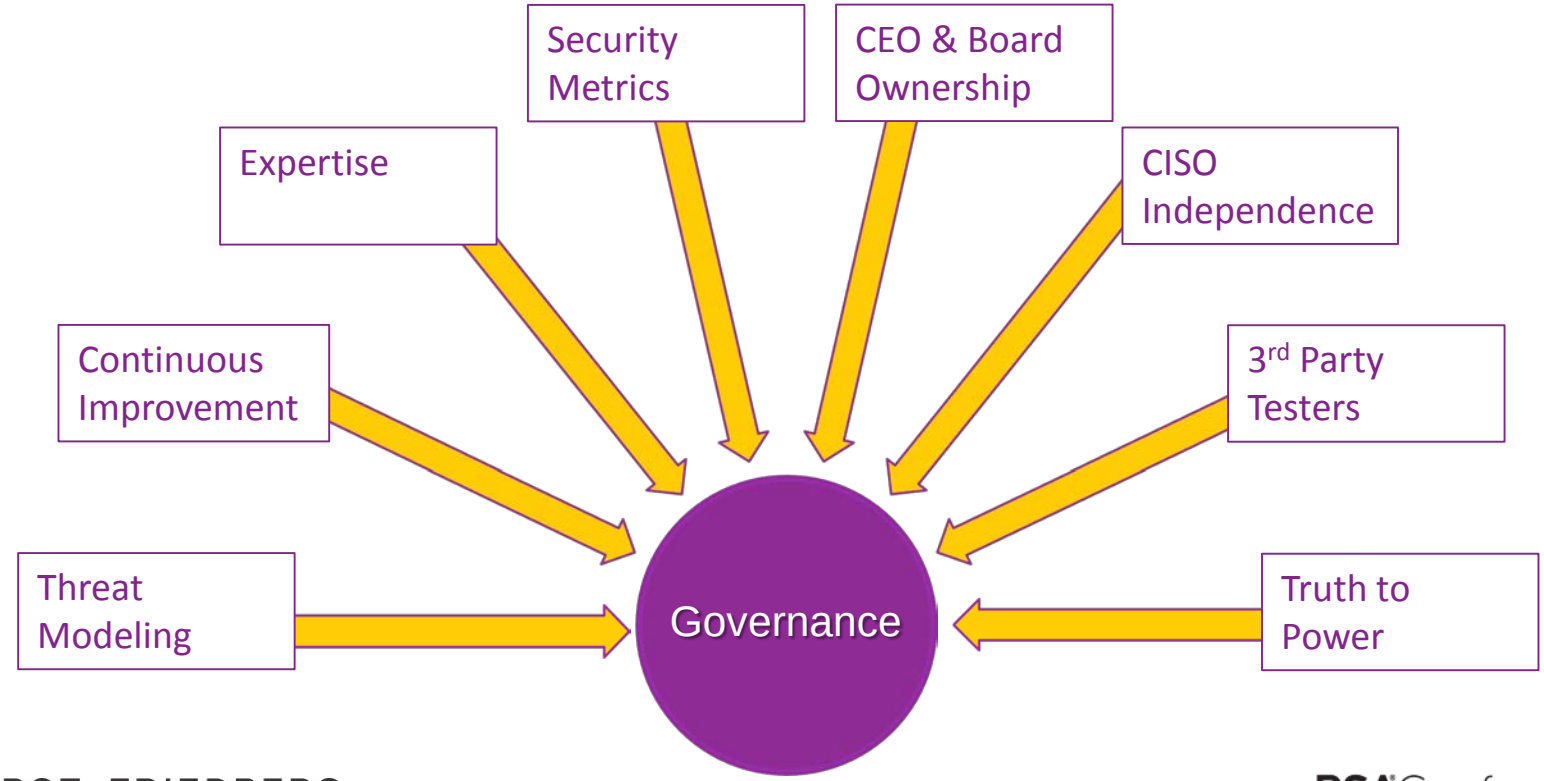
CULTURE

- Create a security culture
- Execute awareness & education program

DATA & ASSET CLASSIFICATION

- Know your most Valuable Assets and where they reside
- Deploy your most sophisticated tech to most Critical Assets

Governance


Security Metrics
CEO & Board Ownership
Expertise
CISO Independence
Continuous Improvement
3rd Party Testers
Threat Modeling
Governance
Truth to Power

Short & Long-term Steps to Confidence

Checklist: It's Never Too Early to Prepare

- ❑ Develop law enforcement contacts
- ❑ Decide on the order of volatility
- ❑ Determine remediation thresholds
- ❑ Finalize power of attorney contact
- ❑ Backup contacts for critical functions
- ❑ Plan for out-of-band communications
- ❑ Test the timing of log acquisitions
- ❑ Define remote access procedure
- ❑ Provide 24/7 support and select incident response vendor
- ❑ Ensure third party readiness

How to Achieve Confidence?

Short-Term Actions

- **Know your Assets:** Understand what you own or create, track your assets via inventory management and continuously assess risk relative to your assets life cycle
- **Know your People** : Perform background check, assess/manage bad leaver risks and leverage your insider risk program to manage on-going risk with your people/contractors.
- **Be IR Ready:** Select Incident Response ("IR") vendor(s) and contract an IR retainer/develop an IR plan
- **Validate Your Current Posture and Risk Profile**: Conduct regular vulnerability and penetration tests

Longer-term actions

- **Know What You Do Not Know:** Seek Cyber Resilience/triangulate what you think you know
- **Practice Your Offense and Defense:** Simulate scenarios/stress-test solutions using third parties with expertise in advanced attacks and make sure you have the technologies, processes, and skill sets (internal and external) lined up in advance
- **Build Up Your Knowledge:** Build a cross-disciplinary cyber response team/get access to the proper level of expertise
- **Know Your Vendors** strengths and weaknesses
- **Ask for a Seat at the Boardroom Table**

Questions?

E JRambaud@strozfriedberg.com
T +1 212.981.6529
in linkedin.com/in/jbrambaud

About JB Rambaud

- Managing Director at Stroz Friedberg, a global consultancy in cybersecurity, forensic investigations, and due diligence
- Chair of the firm's Security Science Business
- Leads his team in conceptualizing, creating, implementing and delivering innovative and custom tailored security solutions
- Clients include the full spectrum of industries

Before joining Stroz Friedberg, JB served as:

- Head of Information Security, Client Services, at Bridgewater Associates LP, the largest hedge fund in the world
- Chief Risk & Security Officer for Fiserv Card Services, worldwide provider of financial services technology
- Director of Corporate Technology and Security at Cerner Corporation, a healthcare information security provider
- Leader of the consulting security practice at Arthur Andersen, the former "Big Five" accounting firm

RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SEM-01

Reflecting on the Next Generation CISO

MODERATOR: **Evan Wheeler**

Executive Director, Operational Risk Management
DTCC

PANELISTS:

Bruce Bonsall
Principal Consultant
Bruce Bonsall LLC

JB Rambaud
Managing Director
Stroz Friedberg LLC

Julie Fitton
Chief Information Security Officer
EMC Cloud Services

Malcolm Harkins
Global CISO
Cylance Corporation

#RSAC

Putting it into action …

- Clarify business challenges with key leaders
- Set aside time for strategic planning that fits the organization
- Know what you don’t know
- Practice your offense and defense
- Make time to tune your message and seek coaching
- Don’t forget to assess the organization’s fit during interviews