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

Connect to Protect

SESSION ID: PDIL-W03

# How To Build or Buy An Integrated Security Stack

**Jay Leek**
CISO
Blackstone

**Haddon Bennett**
CISO
Change Healthcare

#RSAC

# Defining the problem




1. Technology decisions not reducing threat
2. Executives not understanding the threat
3. Inability to quantify investments to reduce threat

Blackstone + CHANGE HEALTHCARE™

# Where to begin…



- What are you trying to protect?






- Strategic direction should be defined by the answer…

Blackstone + CHANGE HEALTHCARE™

# Threats and Attack Surfaces



Define the threats to your organization

- Website hack
- Malware
- Insider
- 3rd Party

What is attack surface?

- Employees with email and web surfing access
- Online storefront
- Point of sale retail
- Single database or secret source code

# Create a maturity model based on your needs

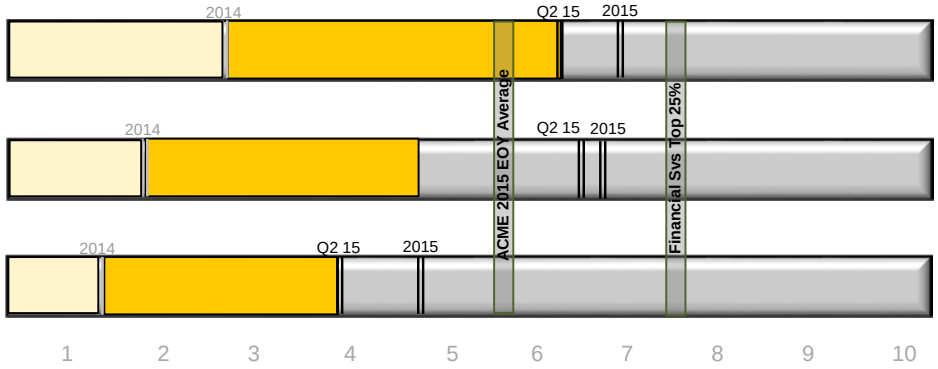
- Identify security controls that mitigate the threats that you have identified
- Measure yourself and create a ‘score’ that clearly shows your maturity level
- Prioritize the key threats your organization must mitigate
- Socialize this with executive leadership for transparency and support of your investments

# Example 1

## Malware
- Mail, Web, Endpoint Antivirus
- Network Advanced Malware
- Threat Analytics and Full Packet Capture etc.

## Data Loss
- Endpoint, Mail, Web Data Loss Prevention
- Mobile Device Encryption
- Digital Rights Management

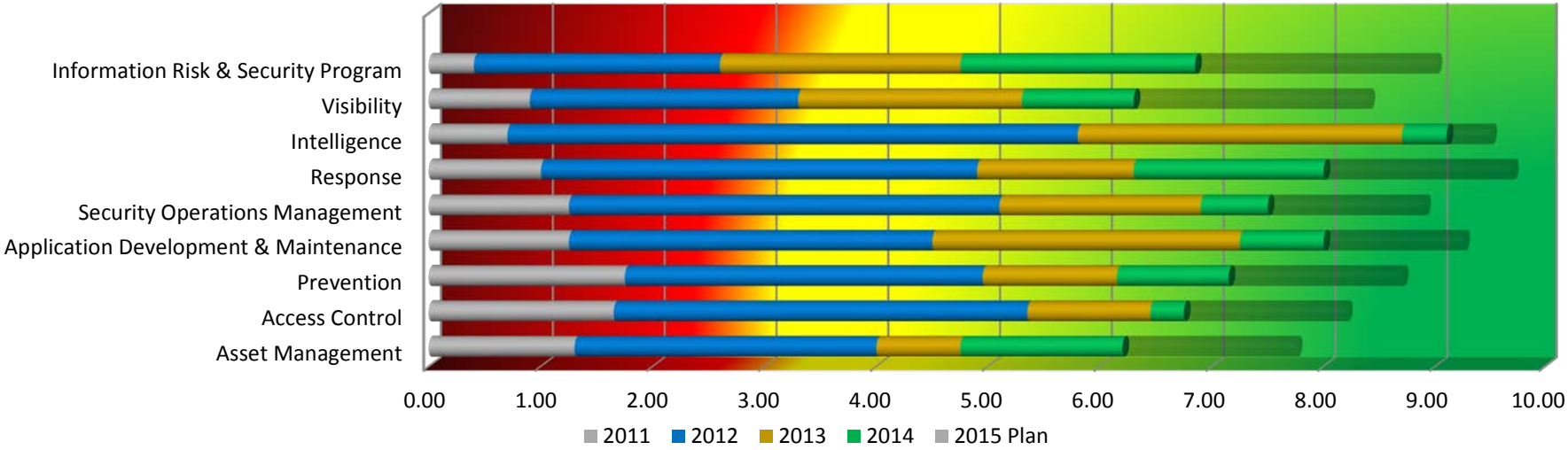
## External Parties
- 3rd Party Risk Assessments
- Vendor Management
- Contract Security




**Benefits**

- Based off of known threats from past breaches
- Clearly shows the top 3 areas that you determine are the most critical
- Visual representation of how and where you need to invest
- Proof of existing maturity and investment payoff over time

# Example 2




Benefits

- Follows ISO framework and NIST Cyber Security Controls
- Shows progress over time to support new investments
- Articulates a security strategy that can be measured and monitored by executives

Blackstone + CHANGE HEALTHCARE™

# Determining Success



- Create a ruler and measure
- Don’t get caught arguing about the measuring stick; focus on left to right movement
- Don’t be afraid to make commitments on the measure
- Understand what success looks like
  - CEO micromanaging your objectives
  - CFO asking how this investment moves me forward
  - Others being asked to create something like your model
  - M&A leader asking how NewCo measures up and what do you need to bring up to the standard

# Selecting the optimal portfolio stack for your company

# Define your architecture




- All tools you invest in must be able to work together, not just with other vendor supplied solutions
- The days of isolated tools and isolated functions have passed us
- Tools must be able to consume intelligence to provide context

# Culture considerations



- You must manage expectations of your end users



- Culture awareness needs to be considered
- Government level security is not always necessary

- Don't underestimate the amount of education it will take for certain security technologies


Blackstone + CHANGE HEALTHCARE™

# Testing and deployment

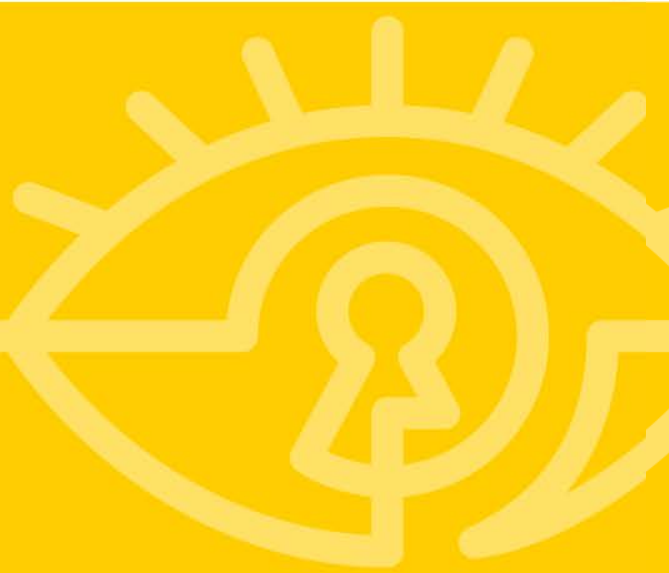


# Truly adding value

# Ensure company viability



Blackstone + CHANGE HEALTHCARE™



# Implementation and architecture

# Understand your risk profile

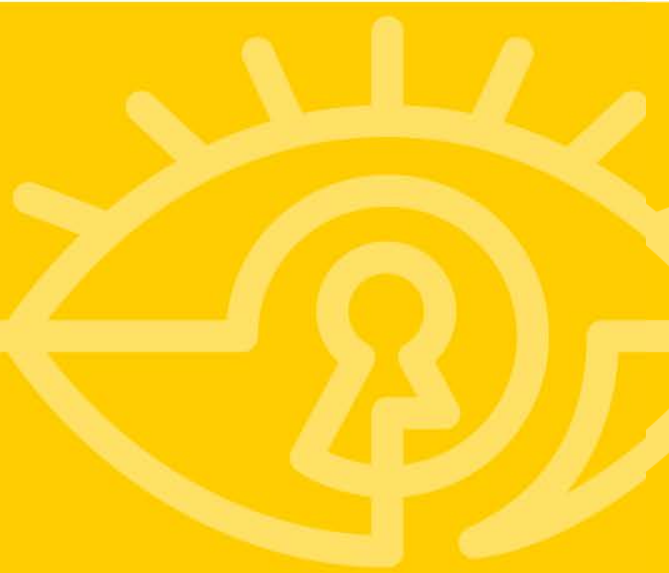


- Not every company is highly regulated or driven by strict customer demands
- Your profile may not lend itself to full data loss prevention blocking on all channels and disallowing any remote access
- Don’t over prescribe as credibility is key to success

# Team

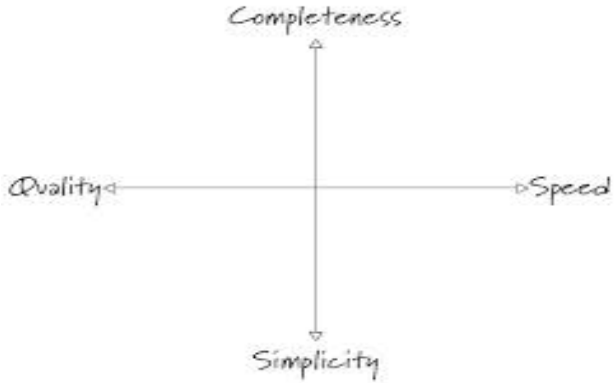


- What are your current talent capabilities
- Certain tool sets lend itself to trusting the protection provided vs. having the skillset to validate and constantly tweak
- If you build vs buy, consider cross training capabilities and retention of the talent to maintain



# Understanding the trade-offs

# Ease of execution

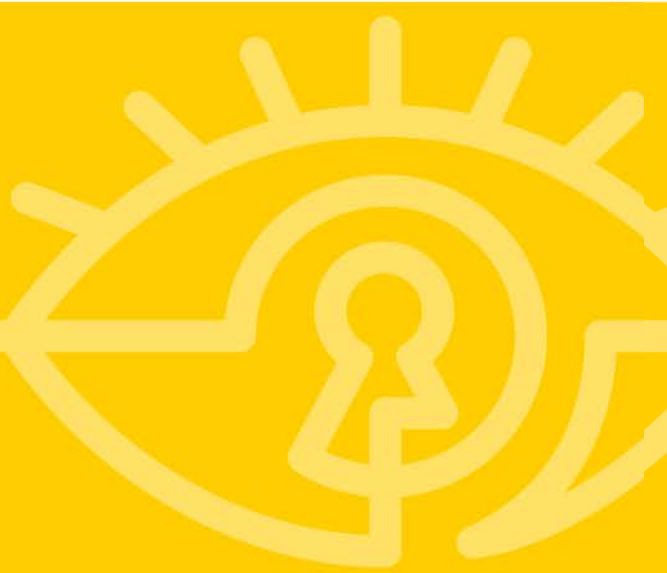




# Communication across teams



- Most security technologies have a tremendous dependency other non-security technologies
- Agent deployments, in-line network gear, email flow integration
- Must consider other teams during the selection process and get their buy-in

# Vendor management



# Case Study:
# Blackstone Security Stack

# Mission Statement



In response to the ever evolving threat landscape

we recommend upending the traditional security paradigm:

**prevent, detect and react**

and embracing an approach that balances prevention with:

**Enhanced Visibility, Situational Awareness & Response**

combined with a business oriented approach to

Information Risk & Security

# Key Value Drivers

- The Blackstone Security Stack is a methodology that security leaders can use as reference guide and/or blueprint aid them in making decisions about their information risk & security program.
- The Blackstone Security Stack provides:
  - Security Guidance / Blueprint for guidance and technical security architecture that leans on ISO 27001 and the NIST Cyber Security Framework
  - Support in justifying purchase of security solutions, services, and SW/HW
  - A framework for budgeting, resourcing and other needs which enables benchmarking across companies
  - Flexibility enabling each security leader to adapt the security stack to properly protect their organization aligned with unique organization risks, budget, and needs

# Addressing the challenging questions

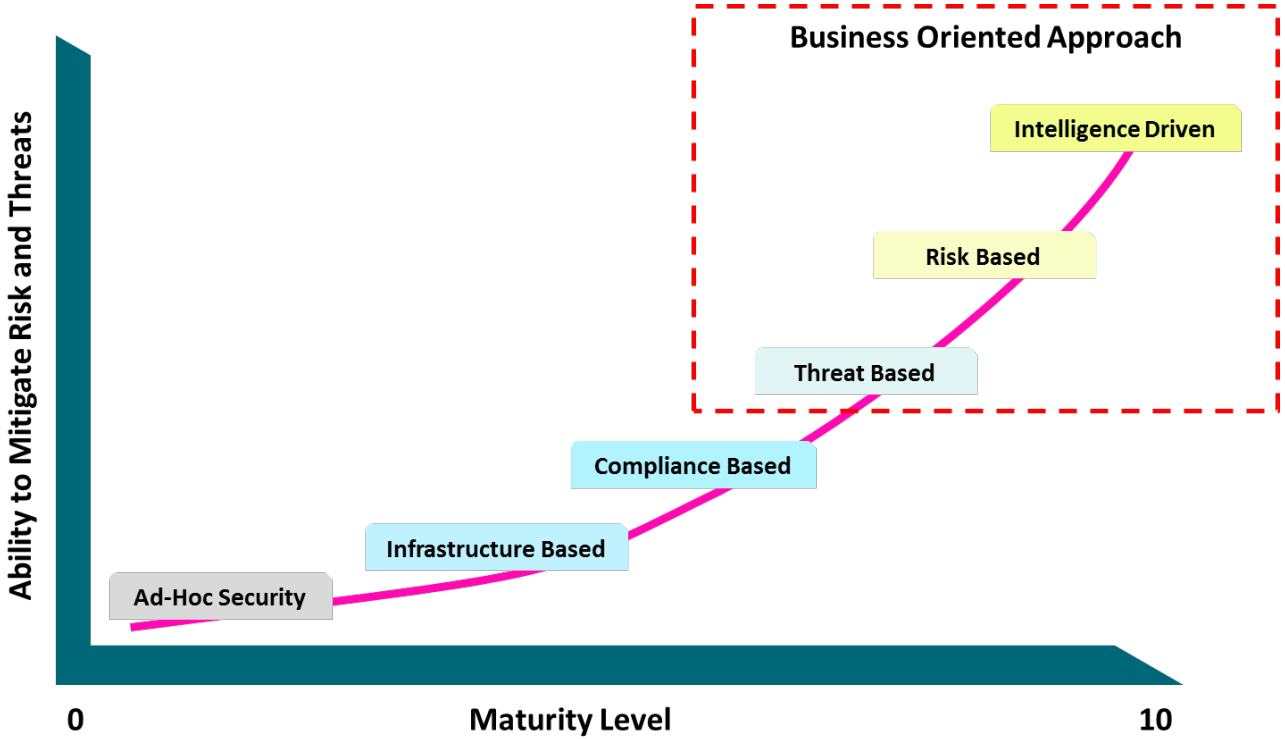


- The Blackstone Security Stack should help answer common questions
  - What are my key threats?
  - Have I been compromised?
  - Am I making the right security investments at the right time?
  - What data do I need to inform and influence positive security outcomes?
  - What is the balance between Being Compliant and Being Secure?
  - **Ultimately, do our controls align with our real threats and risks?**


Blackstone + CHANGE HEALTHCARE™

# Information Risk & Security Maturity Model






Blackstone + CHANGE HEALTHCARE™

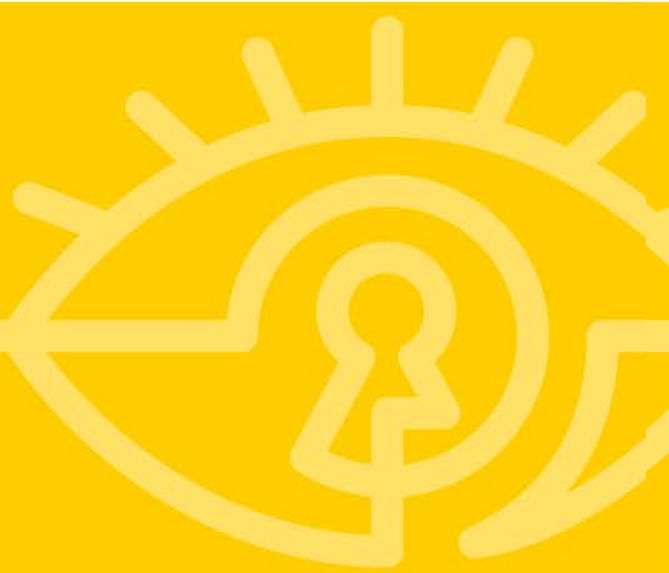
# 100 Day Plan Recommendation



Ensure the following is in place or established:

- Senior management support
  - Budget, resourcing, and collaboration with the technology team
  - Educate as required
- CISO or security leader
- Assessment of the Information Risk & Security Program
  - Identify 5 major gaps or quick wins and close
- Advanced threat detection capabilities on the network or the endpoint
- 2-factor authentication for remote access
- Sufficient technical capabilities and visibility into the environment to determine if the organization may be compromised
  - If not, perform a technical assessment (e.g. Compromised Assessment) by a 3rd party
  - If so, perform a control / threat assessment by a 3rd party
- Post 100 day Security Strategy / Roadmap
  - 12-18-24 months

Blackstone + CHANGE HEALTHCARE™



# Wrap-up

# Key takeaways



- Define what you are trying to protect & measure
- Get appropriate buy-in from executives
- Find the right tools and services that fits your culture
- Understand your risks and implement
- Report on reduction in risk