

RSA[®]Conference2016

San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: SPO3-W05

Assessing Risk: CSOs and Cyber Insurance



Connect **to**
Protect

David Barton

CISO
Forcepoint
@DWBarton1

Joshua Douglas

CTO
Forcepoint
@DouglasRTN



#RSAC

The Problem

THIRTY PERCENT
OF END-USERS CLICK
THROUGH A MALICIOUS URL
(IN AN EMAIL)
EVEN THOUGH
THEY HAVE BEEN
WARNED
OF THE DANGER

DEFEND

INTELLIGENTLY
ADAPT TO
PREVENT
BREACHES
AND DATA
THEFT

31% OF ORGANIZATIONS
ARE PREPARED TO HANDLE RISK
OF INTERNET OF THINGS

ONE OF THE TOP FIVE
MOST LIKELY HIGH-IMPACT RISKS

DEFEAT

TAKE ACTION
TO CONTAIN
AND CONTROL
THREATS

**THE ANNUAL
FINANCIAL
COSTS**

OF INVESTIGATING
AND MITIGATING SECURITY INCIDENTS
INCREASED SUBSTANTIALLY
THIS YEAR, PARTICULARLY
AMONG LARGE ORGANIZATIONS

CYBERSECURITY

DEFEND

DETECT

DECIDE

DEFEAT

**SIXTY-SIX
PERCENT**
OF ORGANIZATIONS
NEED MORE KNOWLEDGEABLE
AND EXPERIENCED
INFORMATION SECURITY
EMPLOYEES

DETECT

DETERMINE
POTENTIAL
BREACHES
AND THEIR
SOURCES

**24 CYBER
TERRORISM**
PERCENT INCREASE IN

DEFENSE-GRADE CYBERSECURITY
THAT DELIVERS UNIFIED
THREAT INTELLIGENCE

THIRTY-TWO PERCENT INCREASE
BIG DATA ANALYTICS AND BEHAVIORAL PROFILING
BY 2018

ANTI-VIRUS AND
ANTI-MALWARE USE
WILL DECREASE

17
PERCENT
NEXT 3 YEARS

DECIDE

LEVERAGE AN
UNDERSTANDING OF
CONTEXT AND IMPACT

19
PERCENT
INCREASED

USE OF AUTOMATED
FORENSICS TOOLS

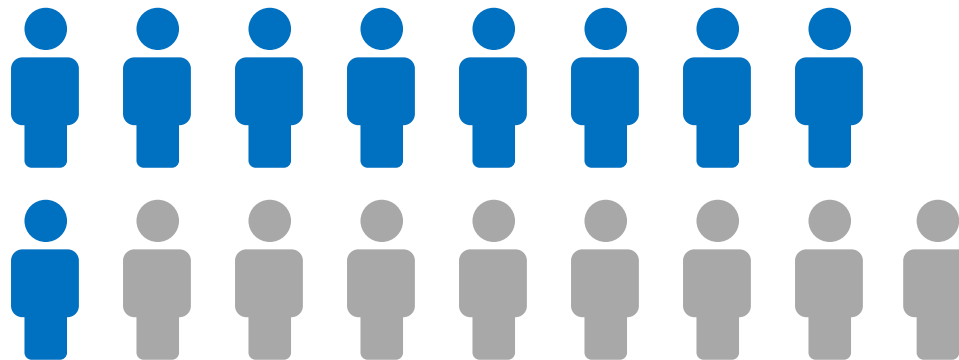


Cybersecurity Skills Gap Grows



#RSAC


2013
2.25 million



2017
4.25 million

*The shortage of skills compounds
the rise in security incidents*

Source: 2013 (ISC)2 Global Information Workforce Study

 = 250,000



Modern Business is All About Safely Connecting Users to Data



#RSAC

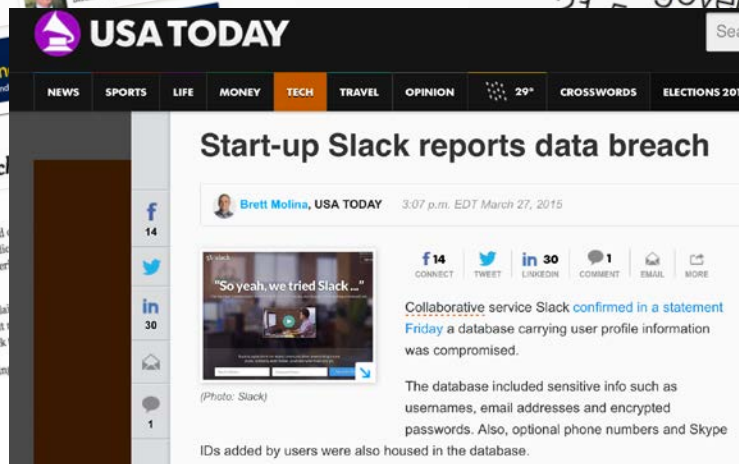


IN THE CLOUD, ON THE ROAD, IN THE OFFICE



2015 Breaches

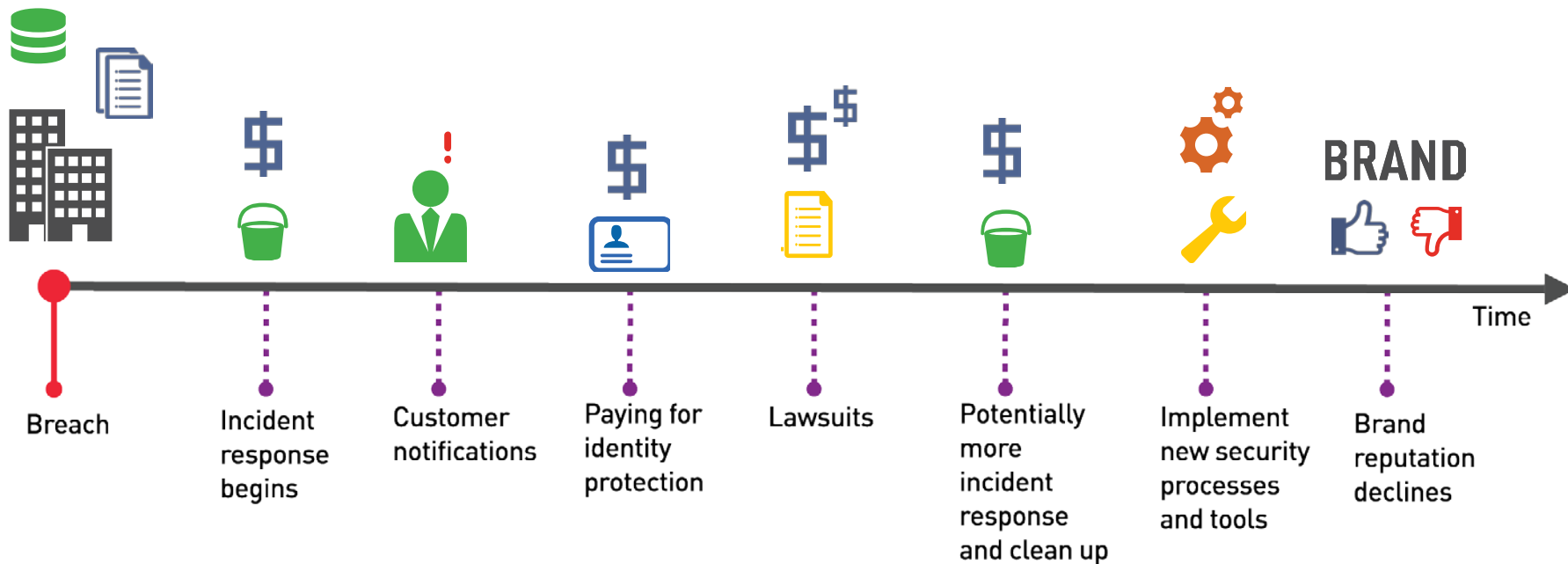
#RSAC



Impacting Business



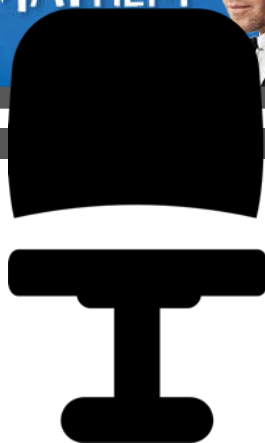
#RSAC



Cyber Mayhem



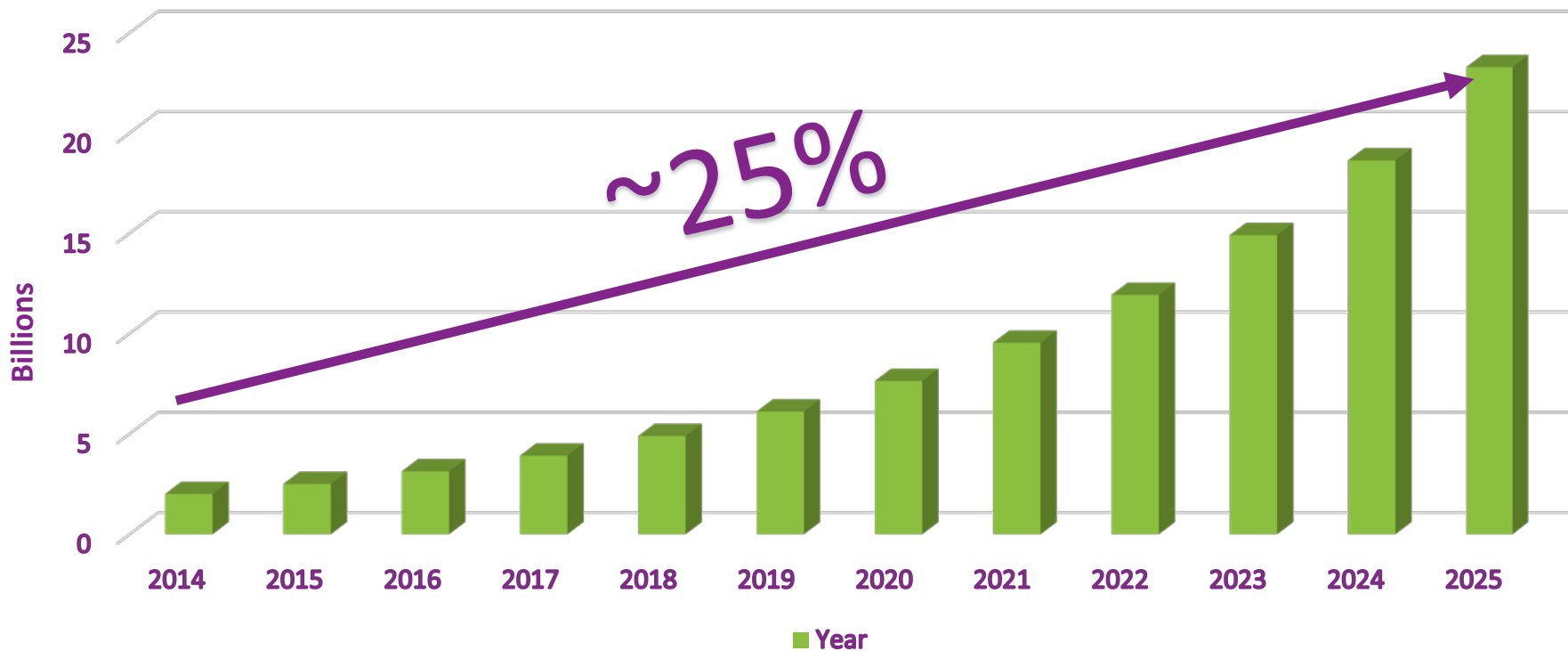
#RSAC



Cyber Insurance Premiums



#RSAC



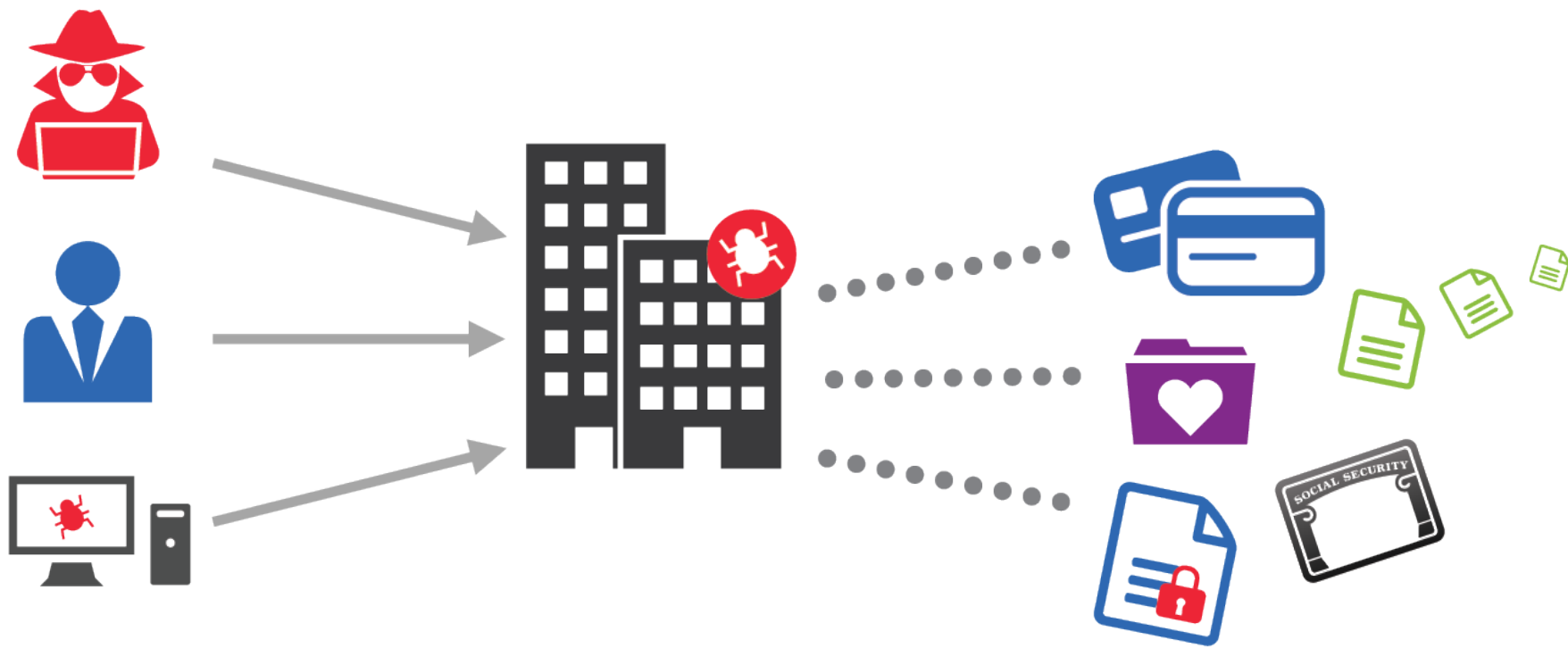
Source: 2015 Allianz, A Guide to Cyber Risk: Managing the Impact of Increasing Interconnectivity
Source: 2015 PwC, Insurance 2020 & beyond: Reaping the dividends of cyber resilience



Liability Protection



#RSAC

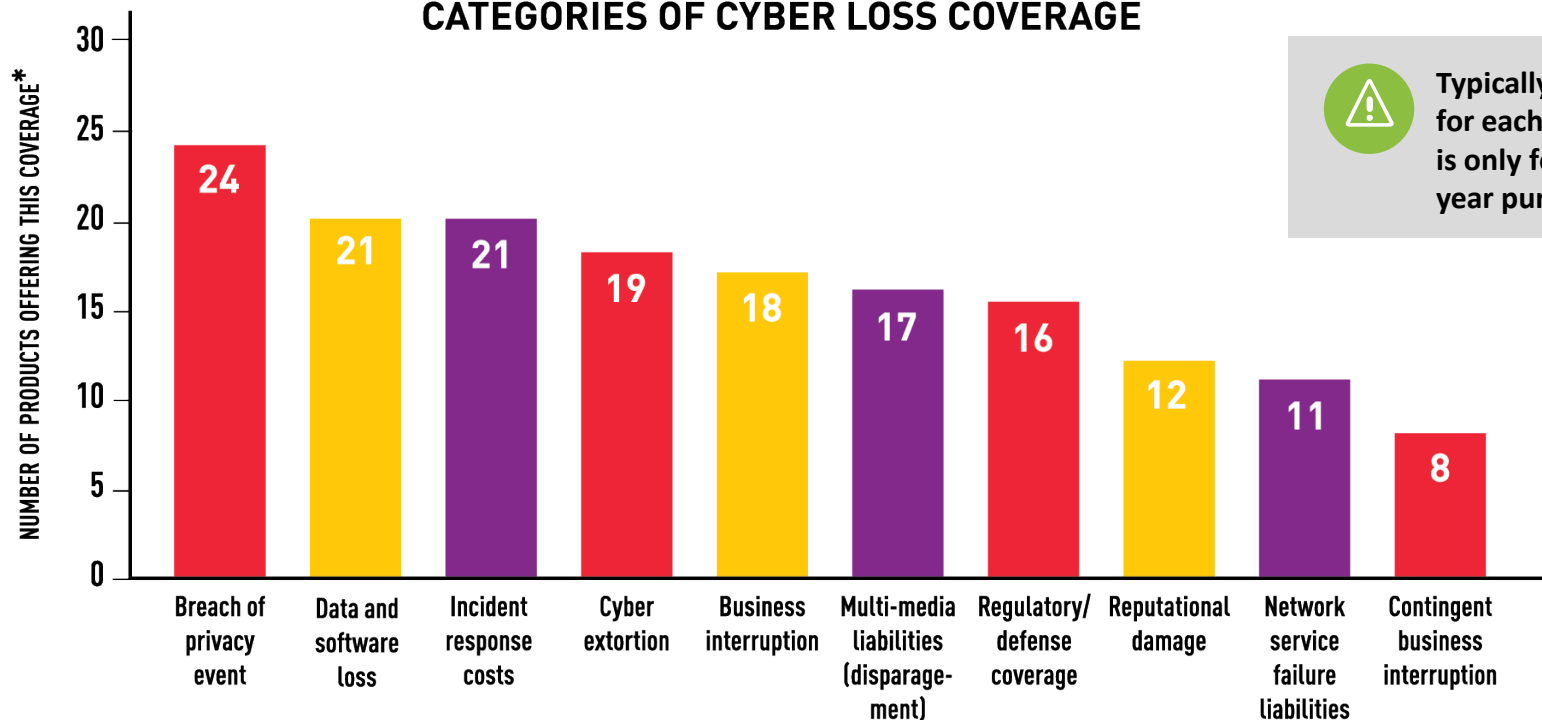


Cyber Insurance Spectrum



#RSAC

CATEGORIES OF CYBER LOSS COVERAGE



Typically coverage for each category is only for the year purchased



Source: 2015 Cambridge Centre for Risk Studies, Cyber Exposure Data Schema V0.5

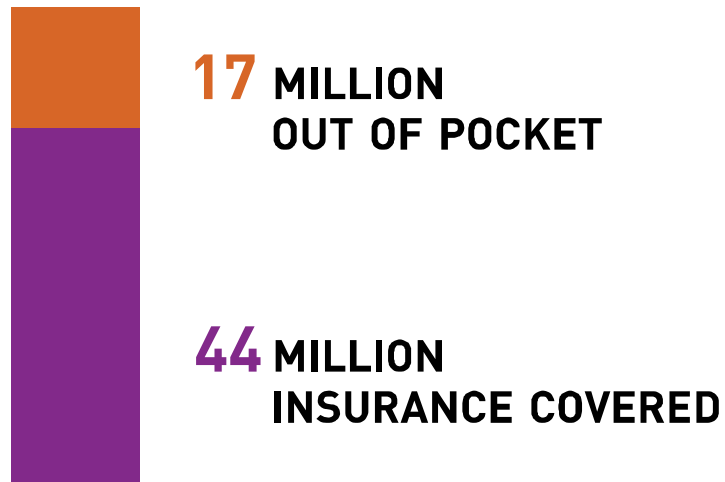
*OUT OF 26 INSURANCE PROVIDERS REVIEWED

Coverage Example



#RSAC

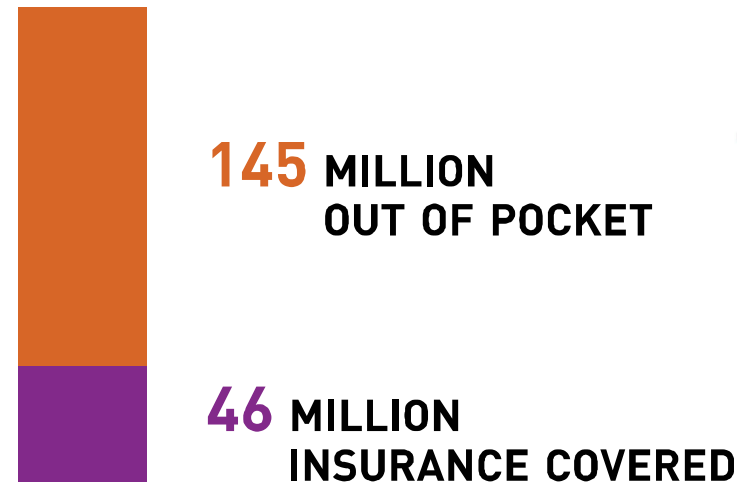
2013 - Target breached in Q4



61 MILLION IN CLEAN UP COSTS FOR 2013



2014 - Clean up continued



191 MILLION IN CLEAN UP COSTS FOR 2014





**\$162 MILLION
OUT OF POCKET***



***WITH DATA BREACH COSTS STILL ROLLING IN**



**INSURANCE ALONE
WILL NOT COVER YOU**



Accurate Actuary Model (Direct Costs)



#RSAC



Insurers claimed 3 problems to an accurate actuary model in a 2014 read out of a working session with DHS on pushing forward the Executive order 13636



Acquiring Insurance...



#RSAC

Revenue

Customer
Contracts

Historical
Business/
Claims

Quality
Control

3rd Party
Information

Information
Security

Physical
Security



Cyber Insurance Scores....



Pen Testing, Passive Data Collection & Incident Response Companies are cashing in on the potential market area by partnering with Cyber Insurance Companies.



Not a single one of these are enough for an accurate model for assessing risk and in some cases they are flawed.



A True model for success...



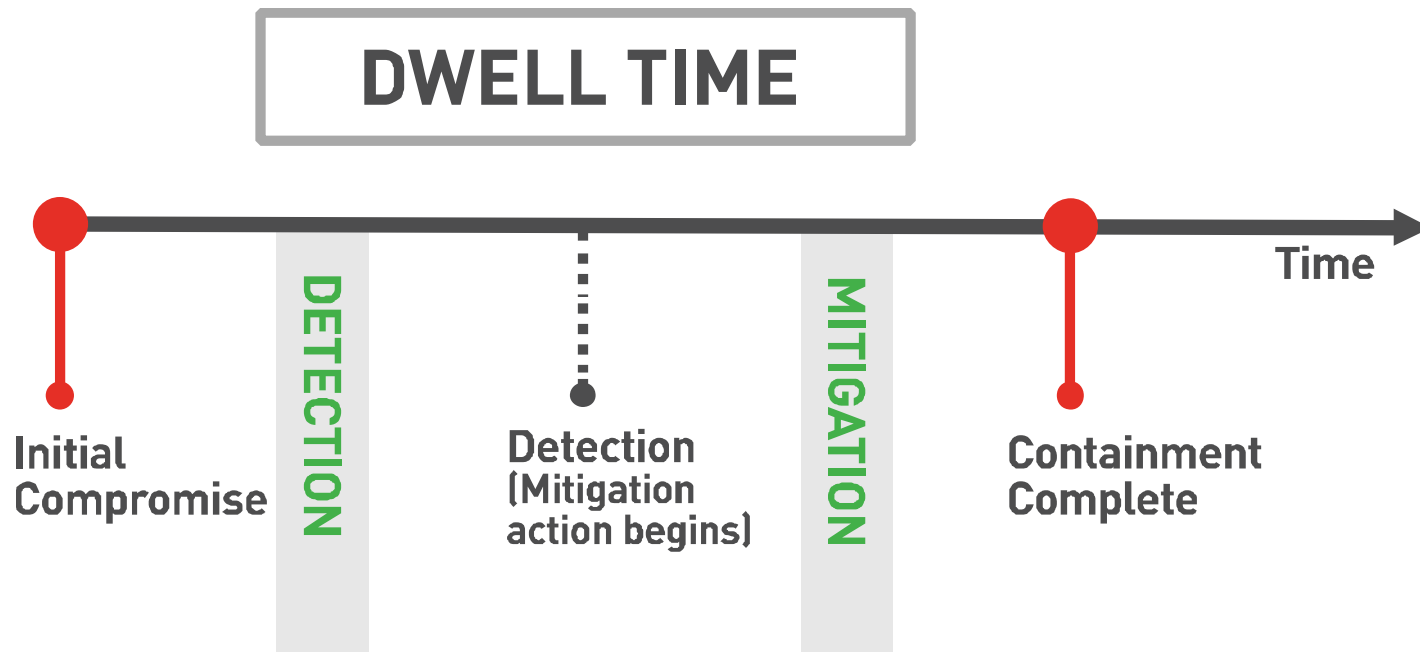
#RSAC



Risk Based Security....



#RSAC



Best Practices – How to Prepare



#RSAC



Immediate Turn Around

- Adopt a security framework and implement it (COBIT, ISO27001, NIST, Cyber Security Framework, etc.)
- Develop and deploy a robust internal security policy
- Ensure a governance process is in place
- Document and retain artifacts of that governance



Continuing Long Term Approach

- Implement a data classification program
- Discover and document data locations
- Implement Data Theft Prevention tools to protect critical data
- Deploy tools to detect and protect against Insider Threats
- Deploy tools to provide full visibility



Framework in Action



#RSAC

Forcepoint Security Framework	Cyber Security Framework	Things to Consider	Mitigating Controls
Defend	Identify & Defend	What assets need protection? What safeguards are available?	Data Discovery Data Classification NGFW Encryption Content Filtering
Detect	Detect	What techniques can identify incidents?	NGFW IDS/IPS Insider Threat
Decide	Respond	What techniques can contain impacts of incidents?	NGFW Insider Threat Content Filtering
Defeat	Recover	What techniques can restore capabilities?	Incident Response Executive Communications Lessons Learned

