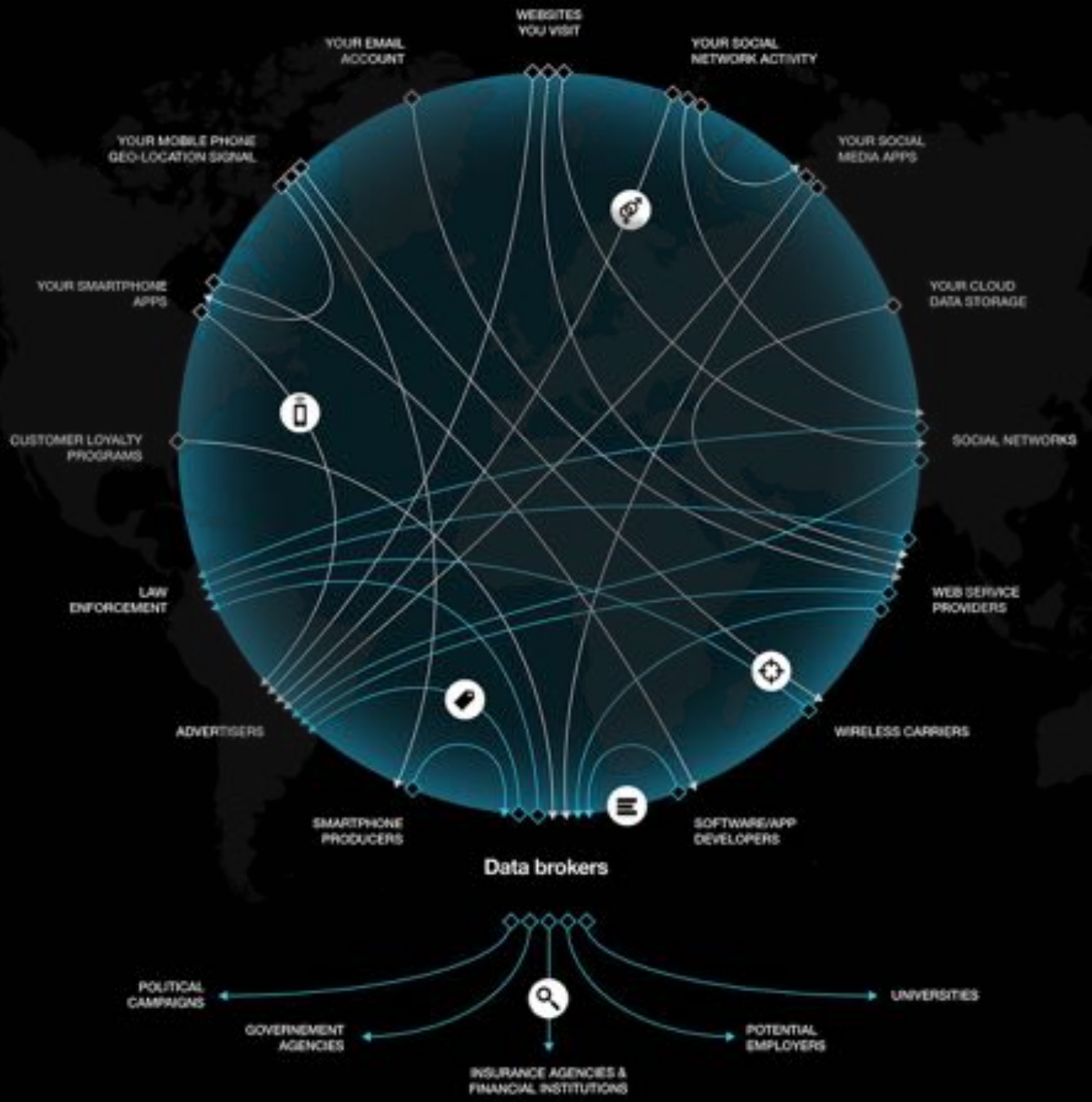
Symantec Incident Response (IR) Services

We are quick moving to a world where everything is connected!



Your Digital Shadow grows with every online interaction!

There's a Vulnerability for everything…

http://www.csoonline.com/article/2835080/data-breach/15-of-the-scariest-things-hacked.html

The Current State of Adversary Defense

RECORD HIGH NUMBERS

429M total identities exposed

9 mega breaches, up 125%

191M identifies exposed in one breach

431M new malware created

ZERO-DAY THREATS

54

all-time high

Top 5 unpatched for 295 days

DIGITAL EXTORTION ON THE RISE

35% increase in crypto-ransom ware

992 devices held hostage each day

OFFENSE IS EASIER

Compromise is no longer if, but when.

DETECTION TAKES TOO LONG

Financial firms take an average of 98 days to detect a data breach and retailers can take up to 197 days

-Ponemon 2015

GAP IN CYBER SKILLS

35% of organizations are unable to fill open security jobs, despite the fact that 82% expect to be attacked this year

-ISACA

RESPONSE TIMES IMPACT THE BUSINESS

The average cost of a data breach is now $3.8M, up from $3.5M a year ago

-Ponemon 2015

Failure to Plan is Planning to Fail

37%

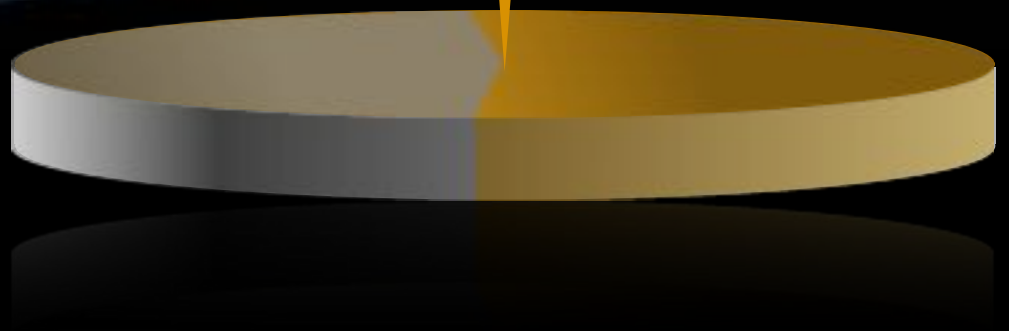
Have not reviewed or updated their response plans since they were put in place

60%

Have a Response Plan

68%

Organizations are not confident that they can deal with the aftermath of a breach.



What Does This Lead To?

Poor Response Times

High Response Costs

Limited Response Effectiveness

Inability to Demonstrate Security ROI

An Example Case Study

[SITUATION:]

- An organization detects a malware outbreak in their environment that is encrypting data, making data inaccessible and slowing the ability for the organization to do business
- Malware spreading to the entire network and bringing operations to a near halt

[RESPONSE:]

- Small internal investigation team typically focused on employee investigations
- IT staff overwhelmed, understaffed, underskilled in Incident Response
- Unable to validate if confidential data has been stolen
- 3rd party forensics firm hired, outbreak is contained, investigation confirms data loss Notification required by breach notification laws

[OUTCOME:]

- ✓ Loss of Confidential Information
- ✓ Loss of Consumer Confidence
- ✓ Brand Damage
- ✓ Post-breach Litigation
- ✓ Operational Impact
- ✓ High Cost Investigation

A Better Approach

People

Qualified, well-trained, cross-functional team with additional expertise on retainer

Technology

Cohesive ecosystem to drive early detection and rapid response

Process

Well constructed, detailed, well-rehearsed response plans

A Better Approach | An Example Case Study

[SITUATION:]

- A customer organization is notified by their MSSP of a potential compromise and is provided a set of indicators to look for to determine if they've been breached and if so, eradicate the attacker from their environment
- Customer has a retainer in place with Symantec for guaranteed response assistance

[RESPONSE:]

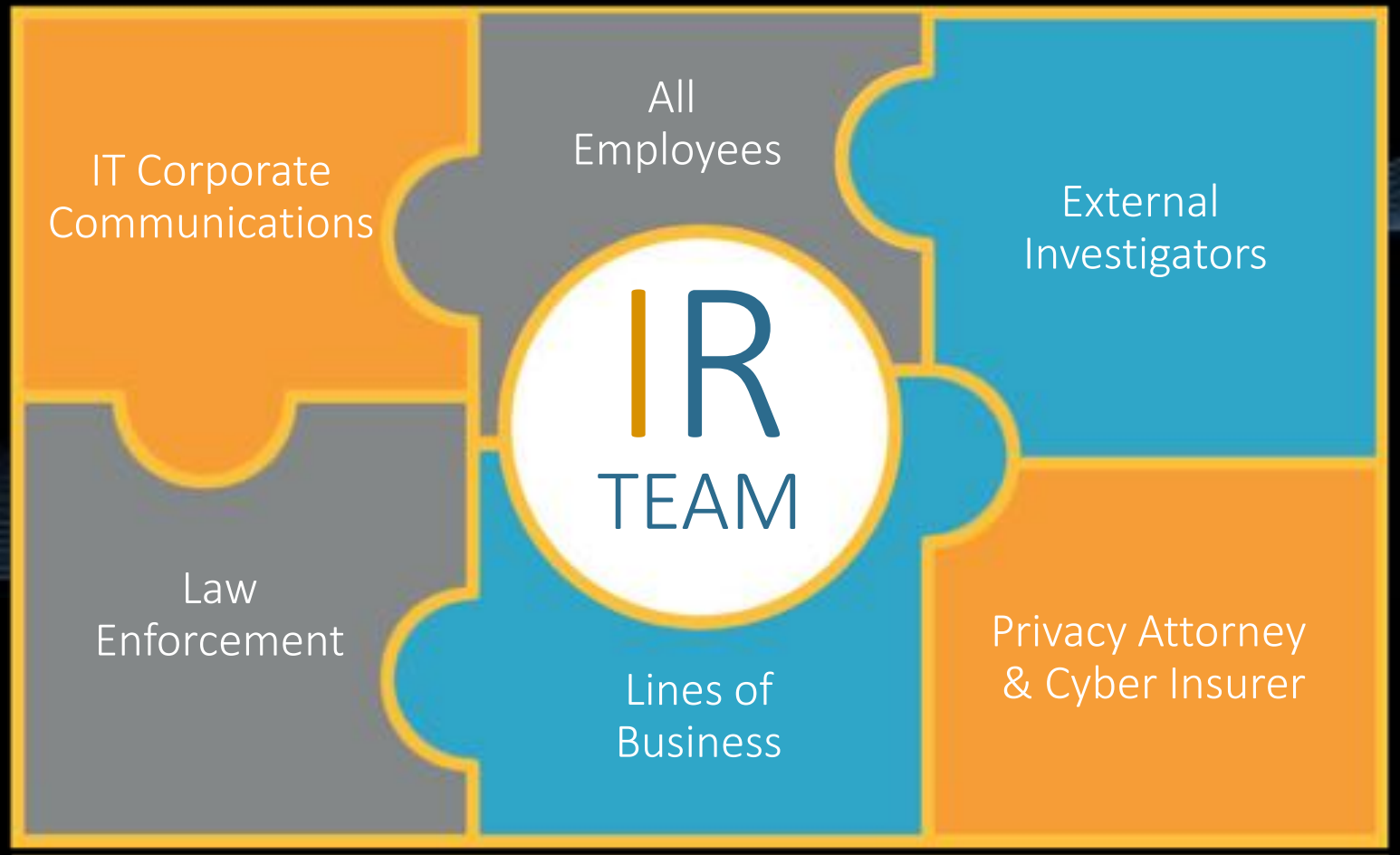
- Symantec IR gathers intelligence from internal repositories based on indicators given and deploys on site
- Symantec IR team arrives and quickly finds an attacker point of entry and implements containment strategy to prevent further damage
- Symantec provides customer detailed recommendations to close attack vectors leveraged by the attacker

[OUTCOME:]

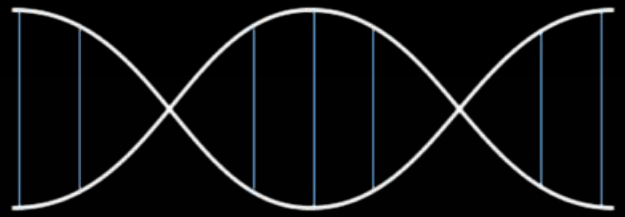
- ✓ Improved Response Times
- ✓ Improved Response Effectiveness
- ✓ Minimal Operational Impact
- ✓ Confidential Data Protected
- ✓ Reduced Risk of Reoccurrence
- ✓ Lower Response Costs

IR is a Team Sport

Expertise and Availability



“Must Have” Responder DNA



Assembling, managing, and preparing an IR team is no small task

EXPERT TECHNICAL SKILLS:

- Operating systems
- Networks
- Applications
- Attack Methods
- Tools
- Log Analysis
- Forensics
- Live response

EXPERT MANAGEMENT SKILLS:

- Thrive under pressure
- Guide risk management decisions
- Understand legal and regulatory implications of various breach scenarios

The Cyber Skills Gap

“By 2020, security industry will be short 1.5 million information security professionals, with this shortage interestingly cited by half of cyber-security staff as a key reason for data breaches (48%).”

-(ISC)²

Proven Process

We Must Plan For Failure

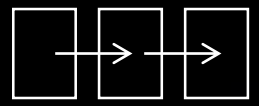
[THE PLAN:]

- ✓ All key policy, process, and roles documented
- ✓ Everyone trained on performing their role
- ✓ Specific playbooks for likely scenarios
- ✓ Technical response plans for all key systems
- ✓ Routine testing of plans performed

How Can We Help?

How Symantec Can Help

Cyber Readiness Services

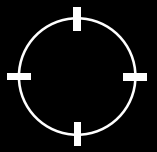


IR Plan and Program Development

- Response Plan Needs & Gap Analysis
- Customized response playbooks for key incident types
- Define IR team roles and responsibilities
- IR team capabilities inventory
- Communications flows and notification procedures

IR Tabletop Exercises

- Assess IR plan effectiveness and IR team ability to execute
- Train response teams to build “muscle memory”
- Identify plan gaps & identify areas for improvement before an incident occurs



Advanced Threat Hunting Compromise Assessment

- Leverage emerging security intelligence to search for signs of compromise
- Deep inspection of system and network data to identify signs of potential compromise
- Detailed report of findings, guidance for recommended improvements & response support (as needed)

How Symantec Can Help

Emergency Response & Retainer Services

Emergency Response

Advanced on-demand fly to site service for Incident identification, investigation and containment

Proactive Retainer Services

Feature	Standard	Enterprise	Advanced Enterprise
Specialized Service Management	✓	✓	✓
Emerging Threat Reports	✓	✓	✓
Remote Assistance SLA	12 hours	12 hours	12 hours
Call Back SLA	3 hours	3 hours	3 hours
Fly to Site Investigation SLA	Priority Access	48 Hours In Transit	24 Hours In Transit
Pre-paid Flt to Site Incident Investigation	10 days*	30 days*	60 days*
Discounted Pricing for Additional Responders	✓	✓	✓
Ability to use Pre-Paid Time for IR Plan Assessment, IR Plan Development, Tabletop Exercises, IR Training, Advanced Threat Hunting	✓	✓	✓

Why Symantec Incident Response?

Experience Matters

- Team Average of 12 years IR Experience
- 50+ IR Technology Patents Held by Team Members
- Direct Experience in Every Industry Vertical including Public Sector
- Experience with High-Profile Breaches

GLOBAL DELIVERY COVERAGE

- Global 24/7 Triage
- Regional Delivery Teams across Americas, EMEA, Asia Pacific, Japan
- Global Operation
- Easy to buy SLA options with global pre-purchased pool of delivery time

Integration with Cyber Security Services

DeepSight Intelligence — Track and Analyze Adversary Groups and Key Trends and Events around the globe for Actionable Intelligence

Managed Security Services — Detect and Proactively Hunt for Targeted Attacks, Advanced Threats and Campaigns

Incident Response — Respond Quickly and Effectively to Credible Security Threats and Incidents

Cyber Skills Development — Strengthen Cyber Readiness to Build Employee Resiliency and Prevent Sophisticated, Advanced Attacks

Hvala!

Davor Kodrnja

davor_kodrnja@symantec.com
+385 91 2424 106