INTEGRATING CYBERSECURITY AND BUSINESS CONTINUITY FOR INCREASED RESILIENCE

DRJ SPRING 2020
March 15-18, Orlando

1

BRIAN STRONG

Head of Information Risk Training and Awareness, CIT Group, Inc.

- ❑ Member of NFPA 1600 Technical Committee
- ❑ Certified in Risk and Information Systems Controls (CRISC)
- ❑ Certified Protection Professional (CPP)
- ❑ Certified Business Continuity Professional (CBCP)

Contact Information

https://www.linkedin.com/in/brianstrongcbcp/

2

AGENDA

- Cyber Resilience Overview
- NIST Framework
- Alignment using NIST Framework
- Integrating Cyber Security and BCM
- Key Takeaways

3

RANSOMWARE ATTACK
Your personal files are encrypted
Business Continuity Institute
BCI CYBER RESILIENCE REPORT
SUNGARD AVAILABILITY SERVICES

KEY FINDINGS

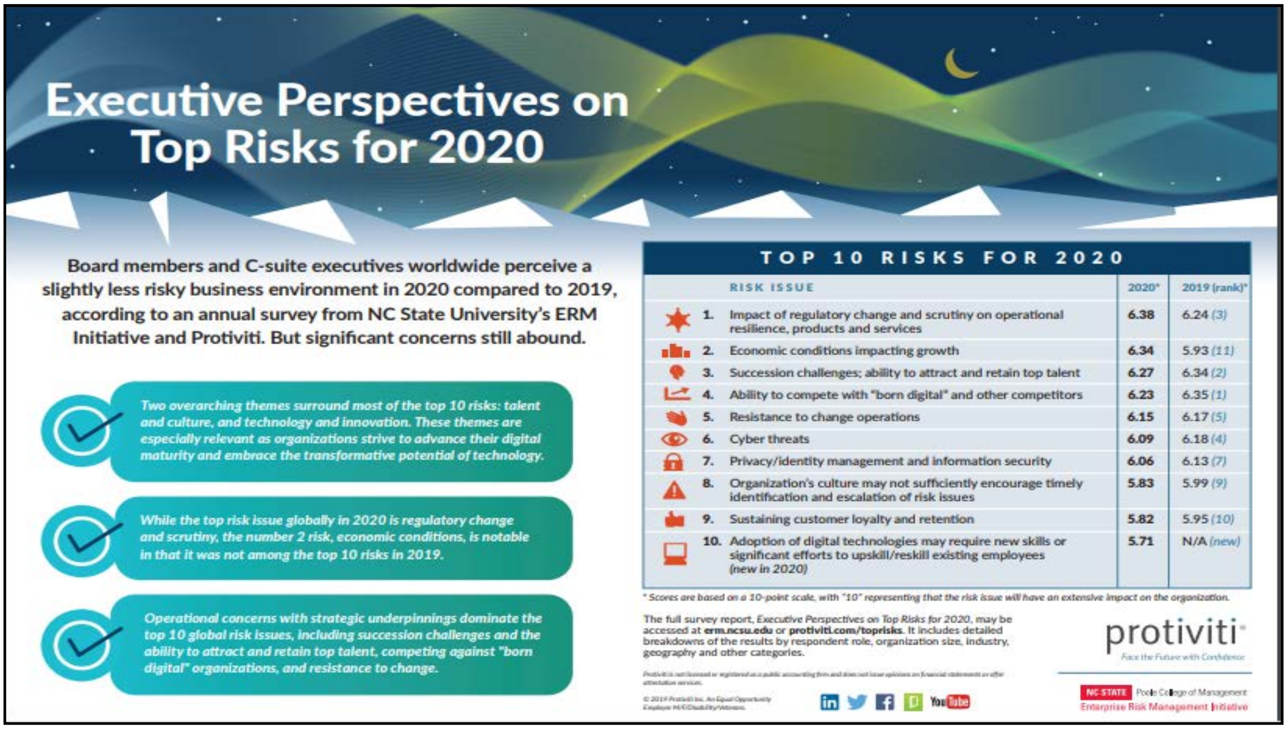
□ The financial cost of cyber-attacks is growing.

□ Reputational damages are also of major concern, 66% of respondents consider reputational damage as the most concerning trend when it comes to cyber security incidents.

□ Moreover, cyber security incidents cannot be considered exclusively non-physical incidents anymore. 46% of respondents consider cyber-attacks with physical security consequences as one of the concerning trends.

□ The cyber threat landscape today is highly complex and rapidly changing and it has become clear that business continuity plays a key role in responding to an incident and ensuring that the organization is able to manage any disruption and prevent it from becoming a crisis.

4



Executive Perspectives on Top Risks for 2020

Board members and C-suite executives worldwide perceive a slightly less risky business environment in 2020 compared to 2019, according to an annual survey from NC State University's ERM Initiative and Protiviti. But significant concerns still abound.

Two overarching themes surround most of the top 10 risks: talent and culture, and technology and innovation. These themes are especially relevant as organizations strive to advance their digital maturity and embrace the transformative potential of technology.

While the top risk issue globally in 2020 is regulatory change and scrutiny, the number 2 risk, economic conditions, is notable in that it was not among the top 10 risks in 2019.

Operational concerns with strategic underpinnings dominate the top 10 global risk issues, including succession challenges and the ability to attract and retain top talent, competing against "born digital" organizations, and resistance to change.

TOP 10 RISKS FOR 2020

	RISK ISSUE	2020*	2019 (rank)*
1.	Impact of regulatory change and scrutiny on operational resilience, products and services	6.38	6.24 *(3)*
2.	Economic conditions impacting growth	6.34	5.93 *(11)*
3.	Succession challenges; ability to attract and retain top talent	6.27	6.34 *(2)*
4.	Ability to compete with "born digital" and other competitors	6.23	6.35 *(1)*
5.	Resistance to change operations	6.15	6.17 *(5)*
6.	Cyber threats	6.09	6.18 *(4)*
7.	Privacy/identity management and information security	6.06	6.13 *(7)*
8.	Organization's culture may not sufficiently encourage timely identification and escalation of risk issues	5.83	5.99 *(9)*
9.	Sustaining customer loyalty and retention	5.82	5.95 *(10)*
10.	Adoption of digital technologies may require new skills or significant efforts to upskill/reskill existing employees *(new in 2020)*	5.71	N/A *(new)*

** Scores are based on a 10-point scale, with "10" representing that the risk issue will have an extensive impact on the organization.*

The full survey report, *Executive Perspectives on Top Risks for 2020*, may be accessed at **erm.ncsu.edu** or **protiviti.com/toprisks**. It includes detailed breakdowns of the results by respondent role, organization size, industry, geography and other categories.

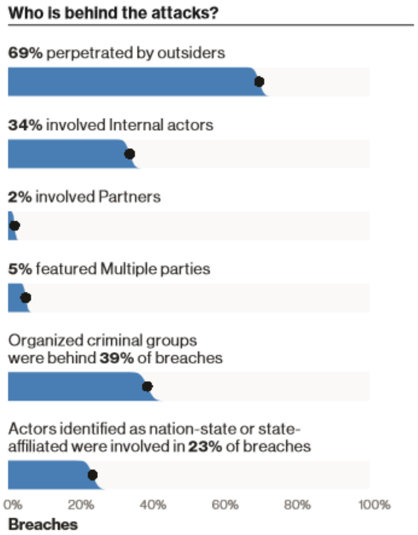
protiviti®
Face the Future with Confidence

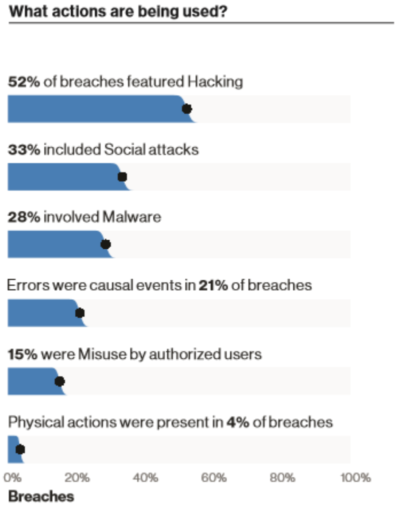
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

NC STATE Poole College of Management
Enterprise Risk Management Initiative

5

THREAT LANDSCAPE

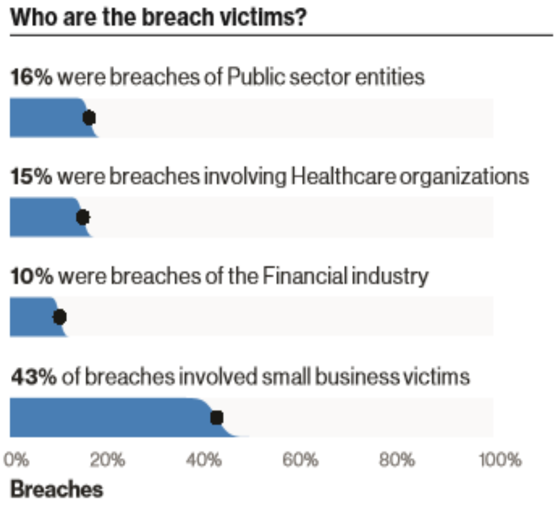




2019 Verizon Data Breach Investigations Report

6

WHO IS AT RISK

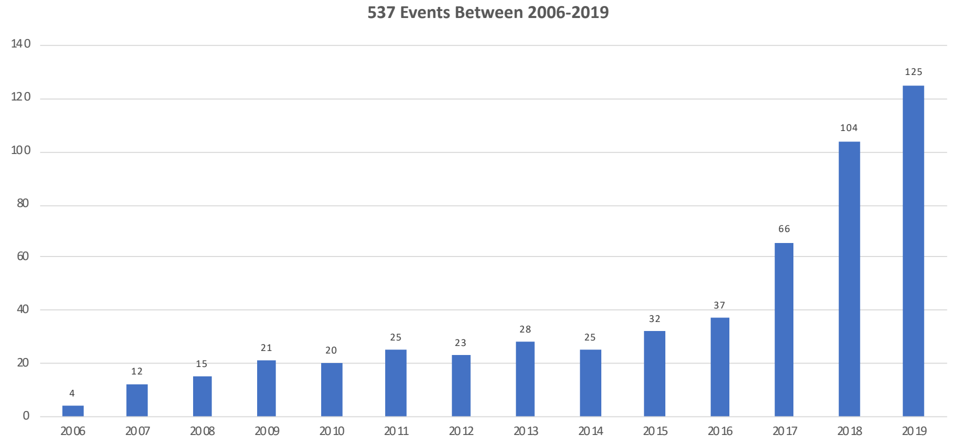


2019 Verizon Data Breach Investigations Report

7

SIGNIFICANT CYBER EVENTS TRENDING

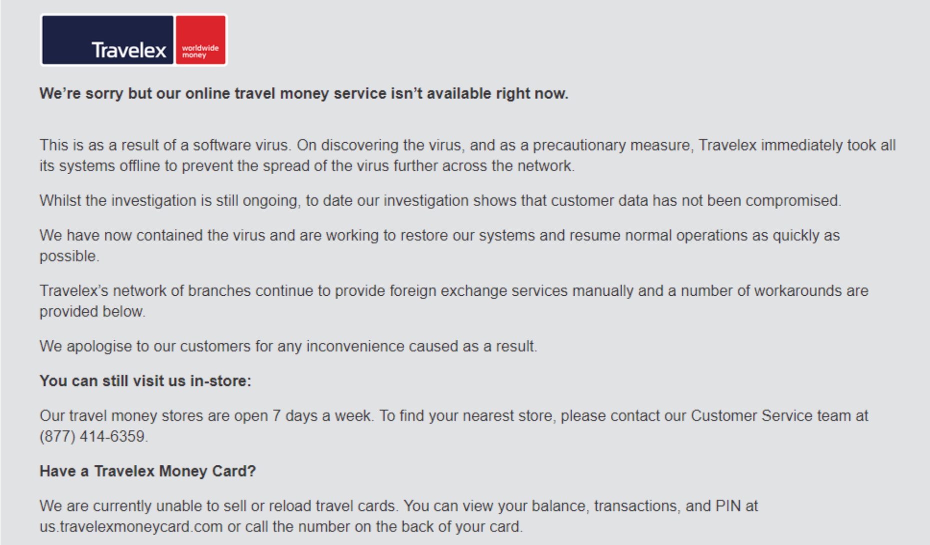
Significant cyber attacks are those occurring on government agencies, defense and high-tech companies, or economic crimes with losses of more than a million dollars.



Source Data: Center for Strategic and International Studies

8

A RECENT CASE STUDY



Travelex worldwide money

We're sorry but our online travel money service isn't available right now.

This is as a result of a software virus. On discovering the virus, and as a precautionary measure, Travelex immediately took all its systems offline to prevent the spread of the virus further across the network.

Whilst the investigation is still ongoing, to date our investigation shows that customer data has not been compromised.

We have now contained the virus and are working to restore our systems and resume normal operations as quickly as possible.

Travelex's network of branches continue to provide foreign exchange services manually and a number of workarounds are provided below.

We apologise to our customers for any inconvenience caused as a result.

You can still visit us in-store:

Our travel money stores are open 7 days a week. To find your nearest store, please contact our Customer Service team at (877) 414-6359.

Have a Travelex Money Card?

We are currently unable to sell or reload travel cards. You can view your balance, transactions, and PIN at us.travelexmoneycard.com or call the number on the back of your card.

Travelex website: 1/13/2020

9

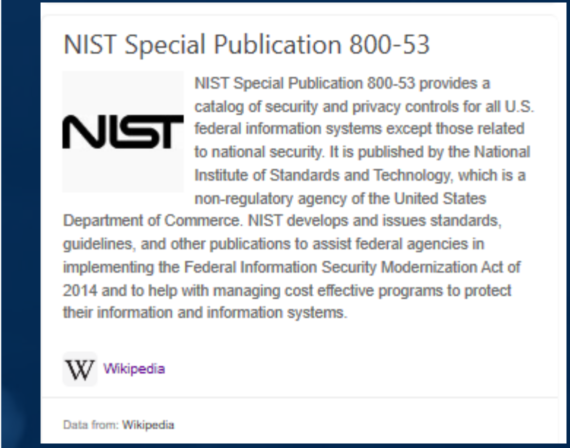
BUSINESS IMPACTS ARE REAL

- Operational
- Reputational
- Audit
- Regulatory
- Legal
- Financial
- Customer Satisfaction
- Stakeholder/Shareholder
- Supply Chain
- Employee Morale

This Photo by Unknown Author is licensed under CC BY-SA

10

INTEGRATION USING NIST 80-53 FRAMEWORK



NIST Special Publication 800-53

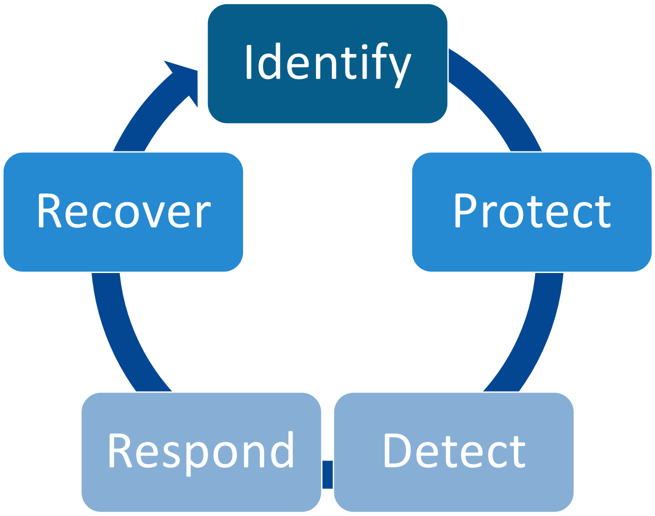
NIST Special Publication 800-53 provides a catalog of security and privacy controls for all U.S. federal information systems except those related to national security. It is published by the National Institute of Standards and Technology, which is a non-regulatory agency of the United States Department of Commerce. NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Modernization Act of 2014 and to help with managing cost effective programs to protect their information and information systems.

Wikipedia

Data from: Wikipedia

11

NIST CYBERSECURITY FRAMEWORK



Identify

Protect

Detect

Respond

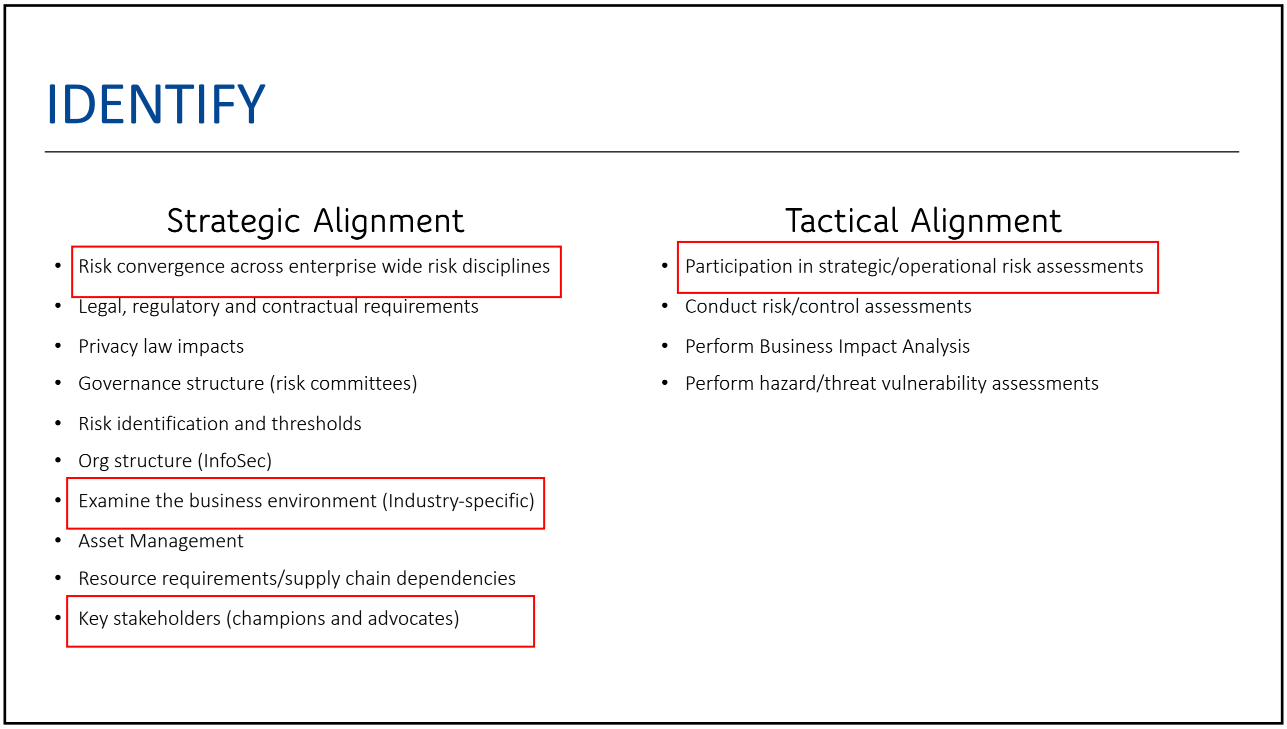
Recover

12

NIST FRAMEWORK ALIGNMENT

FOR INCREASED RESILIENCE

14



IDENTIFY

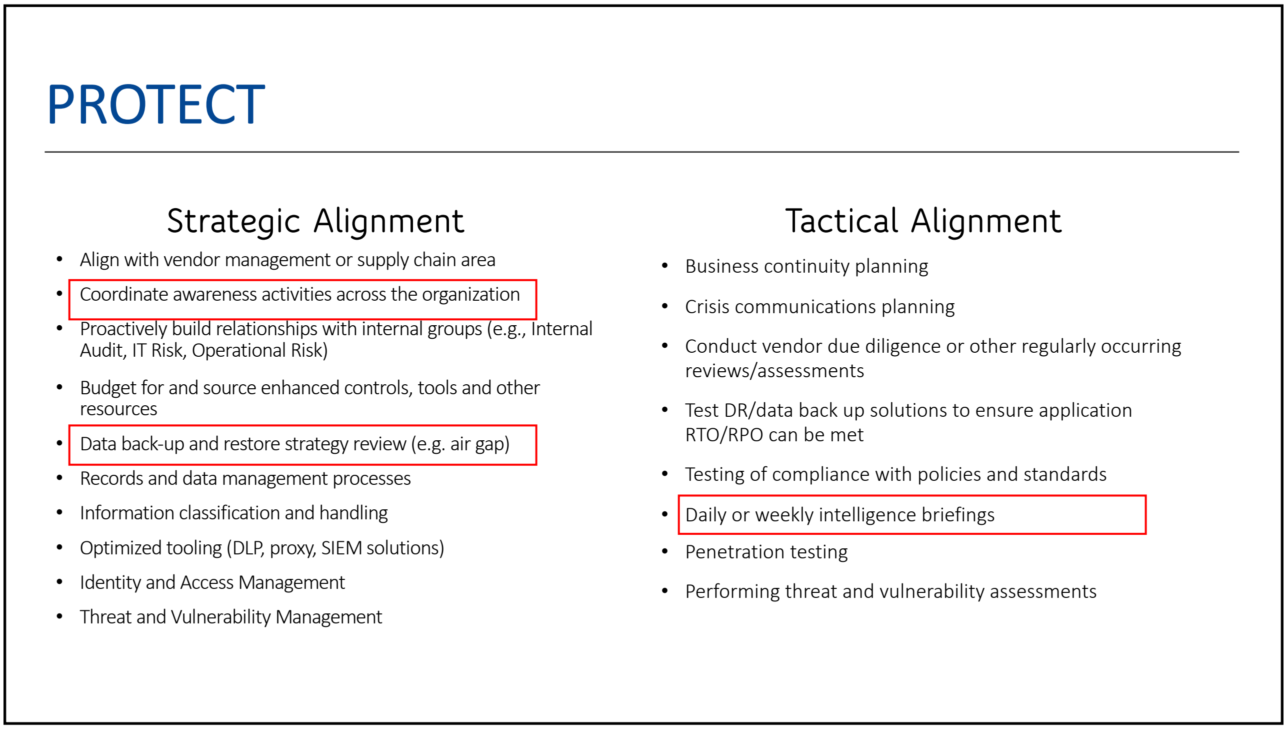
Strategic Alignment

- Risk convergence across enterprise wide risk disciplines
- Legal, regulatory and contractual requirements
- Privacy law impacts
- Governance structure (risk committees)
- Risk identification and thresholds
- Org structure (InfoSec)
- Examine the business environment (Industry-specific)
- Asset Management
- Resource requirements/supply chain dependencies
- Key stakeholders (champions and advocates)

Tactical Alignment

- Participation in strategic/operational risk assessments
- Conduct risk/control assessments
- Perform Business Impact Analysis
- Perform hazard/threat vulnerability assessments

15



PROTECT

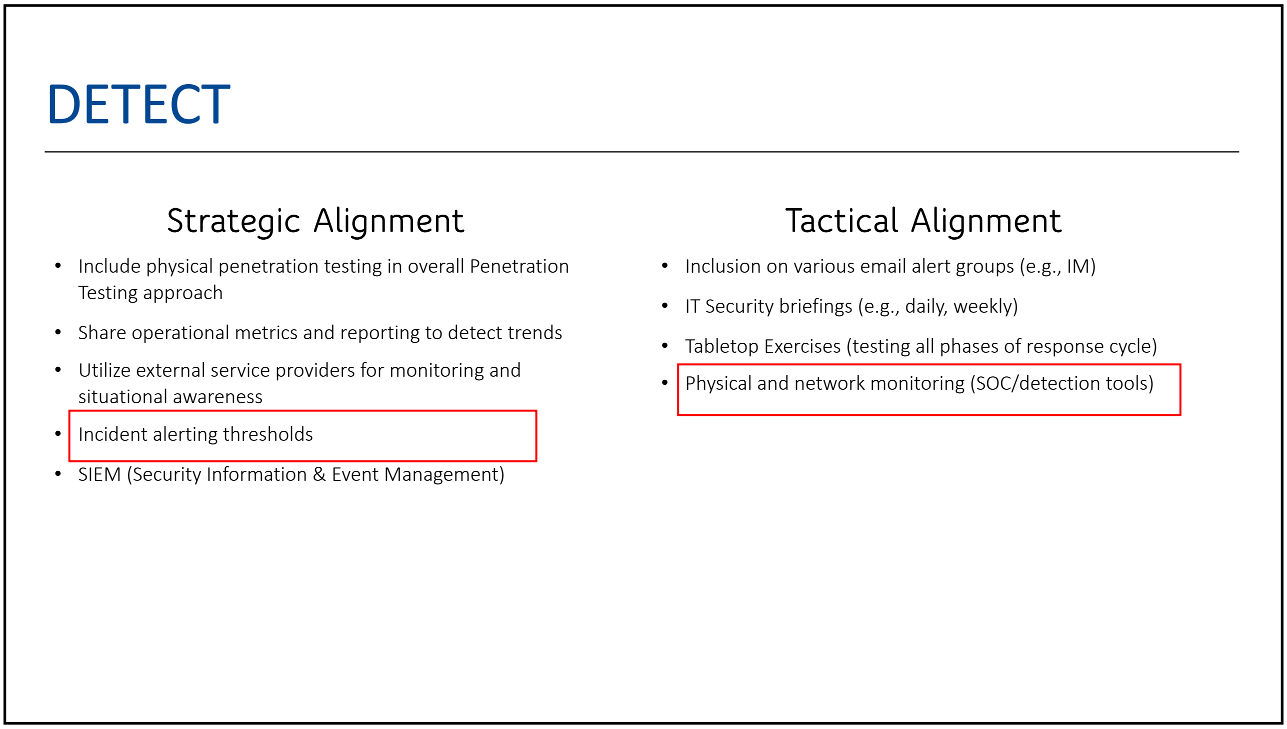
Strategic Alignment

- Align with vendor management or supply chain area
- Coordinate awareness activities across the organization
- Proactively build relationships with internal groups (e.g., Internal Audit, IT Risk, Operational Risk)
- Budget for and source enhanced controls, tools and other resources
- Data back-up and restore strategy review (e.g. air gap)
- Records and data management processes
- Information classification and handling
- Optimized tooling (DLP, proxy, SIEM solutions)
- Identity and Access Management
- Threat and Vulnerability Management

Tactical Alignment

- Business continuity planning
- Crisis communications planning
- Conduct vendor due diligence or other regularly occurring reviews/assessments
- Test DR/data back up solutions to ensure application RTO/RPO can be met
- Testing of compliance with policies and standards
- Daily or weekly intelligence briefings
- Penetration testing
- Performing threat and vulnerability assessments

16



DETECT

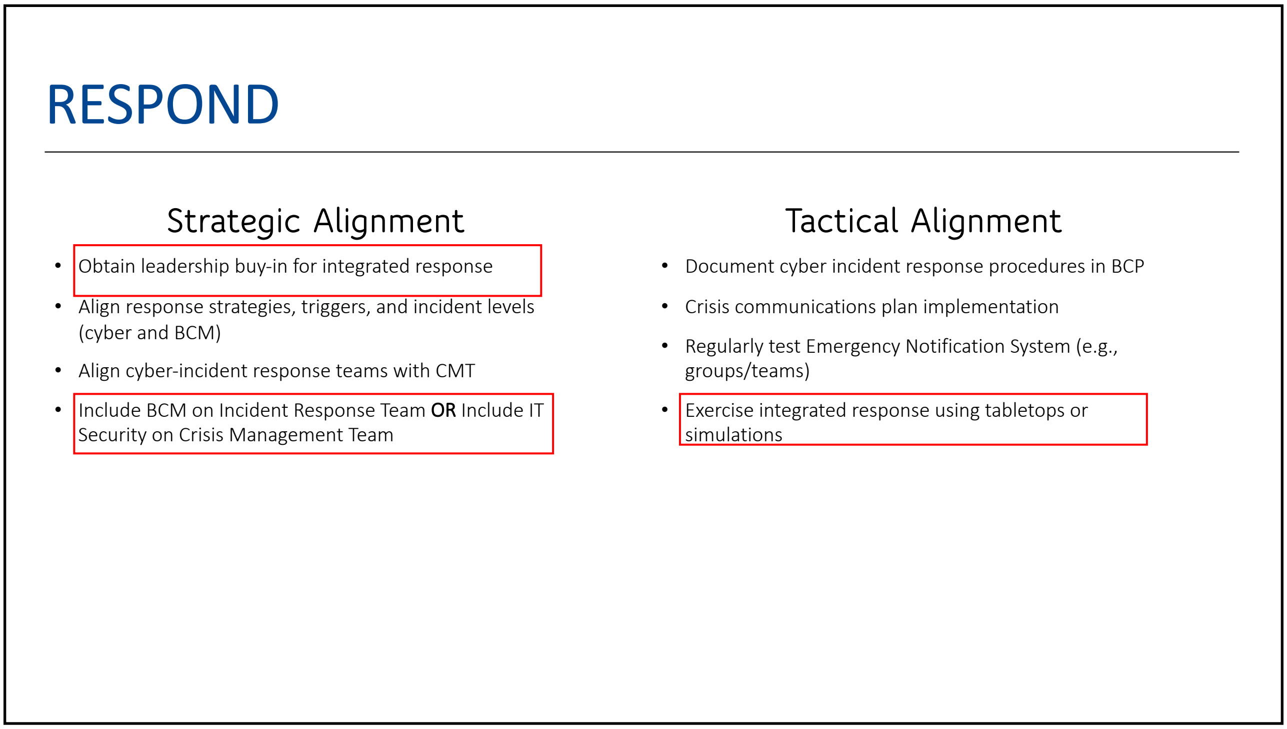
Strategic Alignment

- Include physical penetration testing in overall Penetration Testing approach
- Share operational metrics and reporting to detect trends
- Utilize external service providers for monitoring and situational awareness
- Incident alerting thresholds
- SIEM (Security Information & Event Management)

Tactical Alignment

- Inclusion on various email alert groups (e.g., IM)
- IT Security briefings (e.g., daily, weekly)
- Tabletop Exercises (testing all phases of response cycle)
- Physical and network monitoring (SOC/detection tools)

17



RESPOND

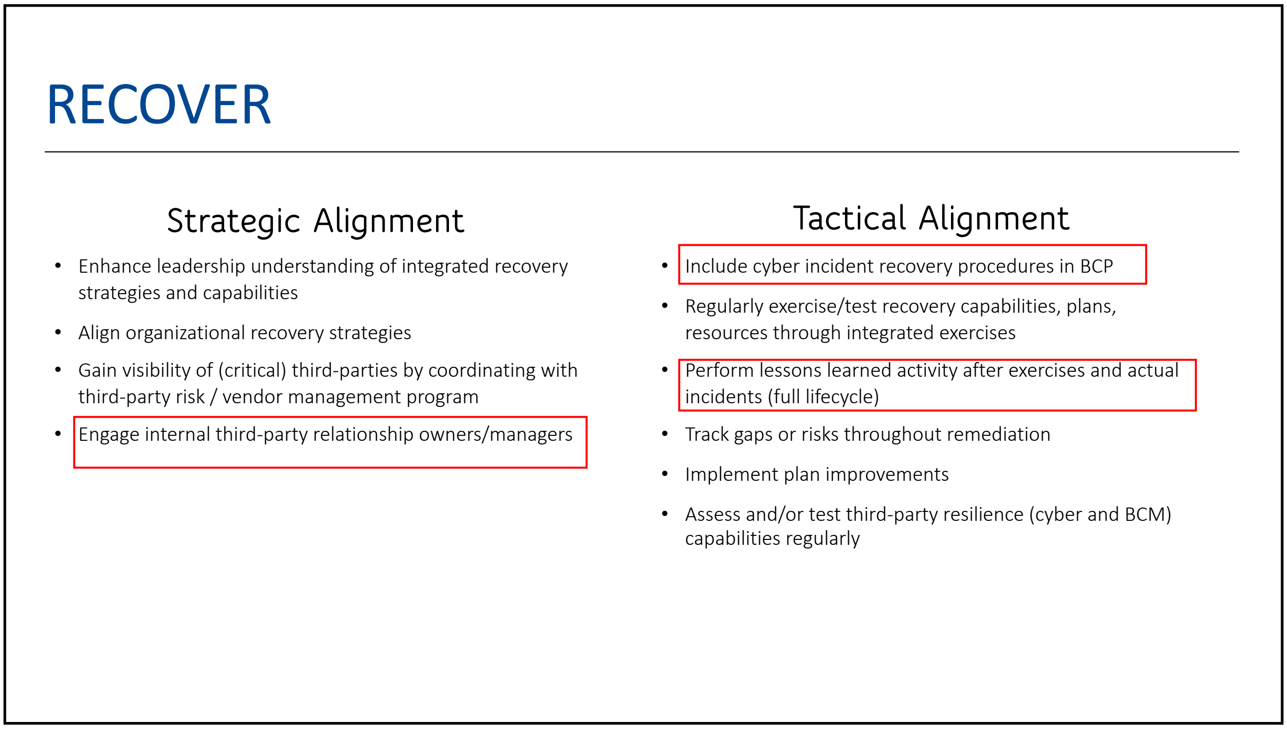
Strategic Alignment

- Obtain leadership buy-in for integrated response
- Align response strategies, triggers, and incident levels (cyber and BCM)
- Align cyber-incident response teams with CMT
- Include BCM on Incident Response Team **OR** Include IT Security on Crisis Management Team

Tactical Alignment

- Document cyber incident response procedures in BCP
- Crisis communications plan implementation
- Regularly test Emergency Notification System (e.g., groups/teams)
- Exercise integrated response using tabletops or simulations

18



RECOVER

Strategic Alignment

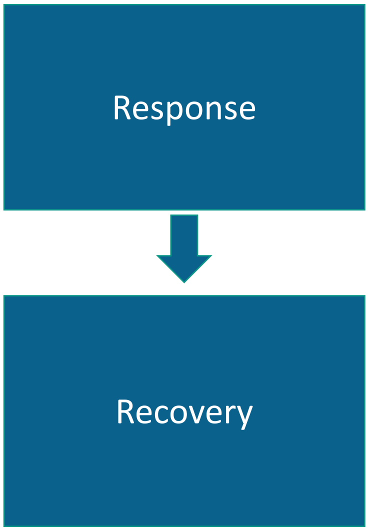
- Enhance leadership understanding of integrated recovery strategies and capabilities
- Align organizational recovery strategies
- Gain visibility of (critical) third-parties by coordinating with third-party risk / vendor management program
- Engage internal third-party relationship owners/managers

Tactical Alignment

- Include cyber incident recovery procedures in BCP
- Regularly exercise/test recovery capabilities, plans, resources through integrated exercises
- Perform lessons learned activity after exercises and actual incidents (full lifecycle)
- Track gaps or risks throughout remediation
- Implement plan improvements
- Assess and/or test third-party resilience (cyber and BCM) capabilities regularly

19

SAMPLE BCP PROCEDURES



Response

1. Contact the IT Security Hotline Immediately
2. Notify your manager
3. Note exactly what you were doing prior to the attack
4. Do not unplug any hardware

Recovery

1. Follow instructions provided by your management and IT Security
2. Perform manual process, if applicable
3. Validate application/system recovery
4. When authorized, validate data integrity

20

KEY TAKEAWAYS

FIND A WILLING PARTNER
Seek internal stakeholders that can be champions or advocates for integration.

SYNERGIZE
Engage stakeholders throughout the process. Seek input where appropriate.

LEVERAGE A FRAMEWORK
Use an existing or adopted framework for integration design.

THINK STRATEGICALLY ACT TACTICALLY
Look at the big picture and then plan for how to operationalize integration efforts.

NO STONE UNTURNED
Be creative. Seek ways to integrate by exploring all possibilities.

PRACTICE, PRACTICE, PRACTICE
After initial integration is finalized, perform a dress rehearsal. Capture lessons learned to improve resilience.

DRJ SPRING 2020
March 15-18, Orlando

21

Thank you

22