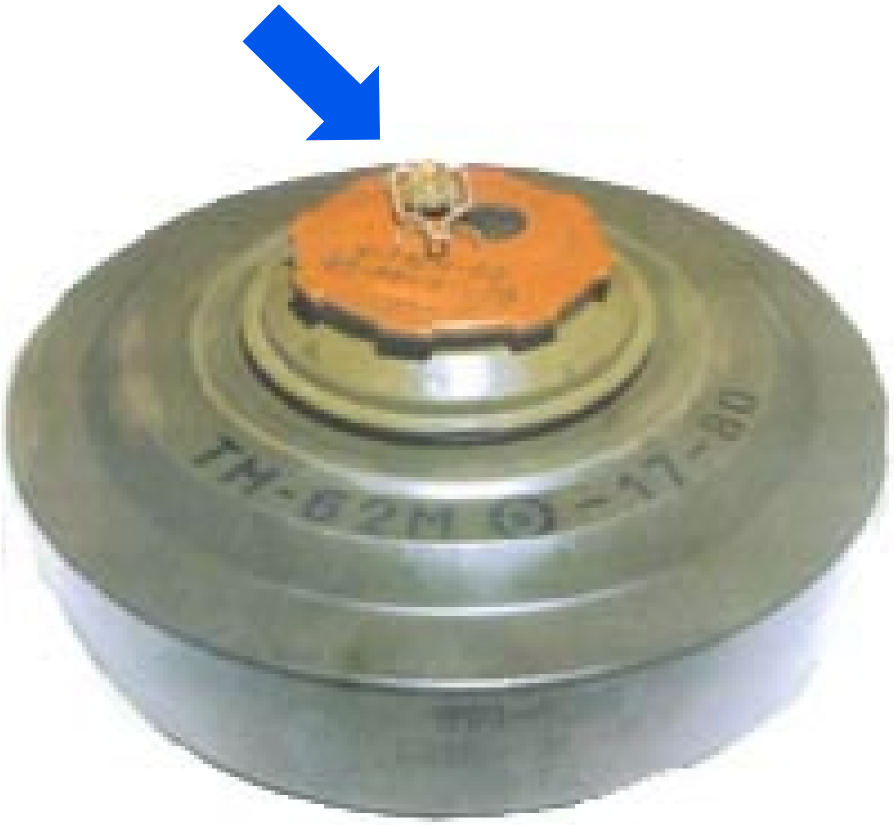
Avoid Landmines with your Backup and Recovery Strategy

Nick Shirk, National Sales Director
Information Security & Technology

jack henry™

Nick Shirk

- BS, Industrial Mgmt – MIS and Finance – Purdue University
- MBA, Finance & Strategy – The University of Notre Dame
- Graduate School of Banking (GSB) – UW Madison
- 20+ years – IT, Dev Ops, Security, Consulting
- 13+ years working with financial institutions
- 6 Years JHA
- Led IT/Operations at a couple financial institutions


ТМ-62М ⊙-17-80

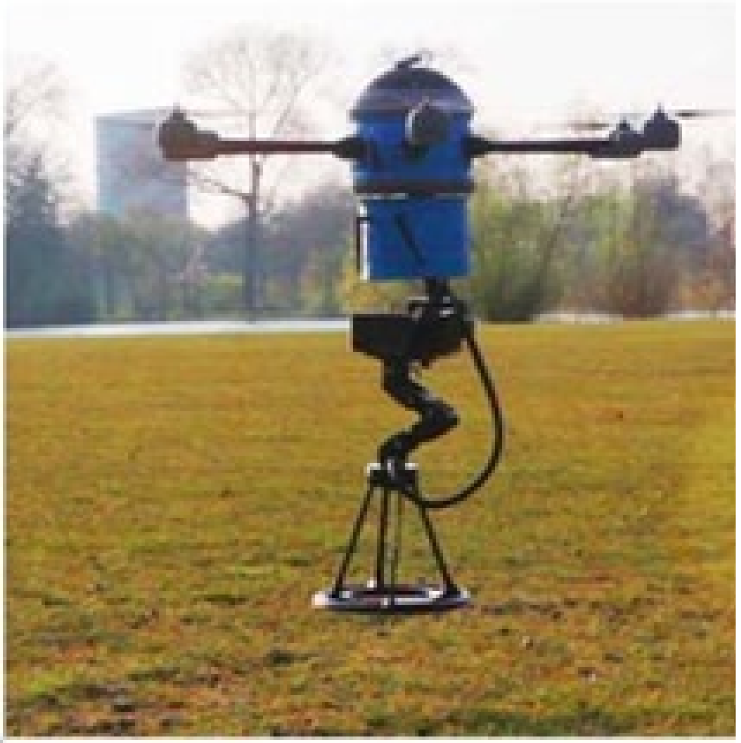
Airborne Demining in 3 Steps

Airborne Demining in 3 Steps

Mapping

Airborne Demining in 3 Steps

Mapping



Detecting

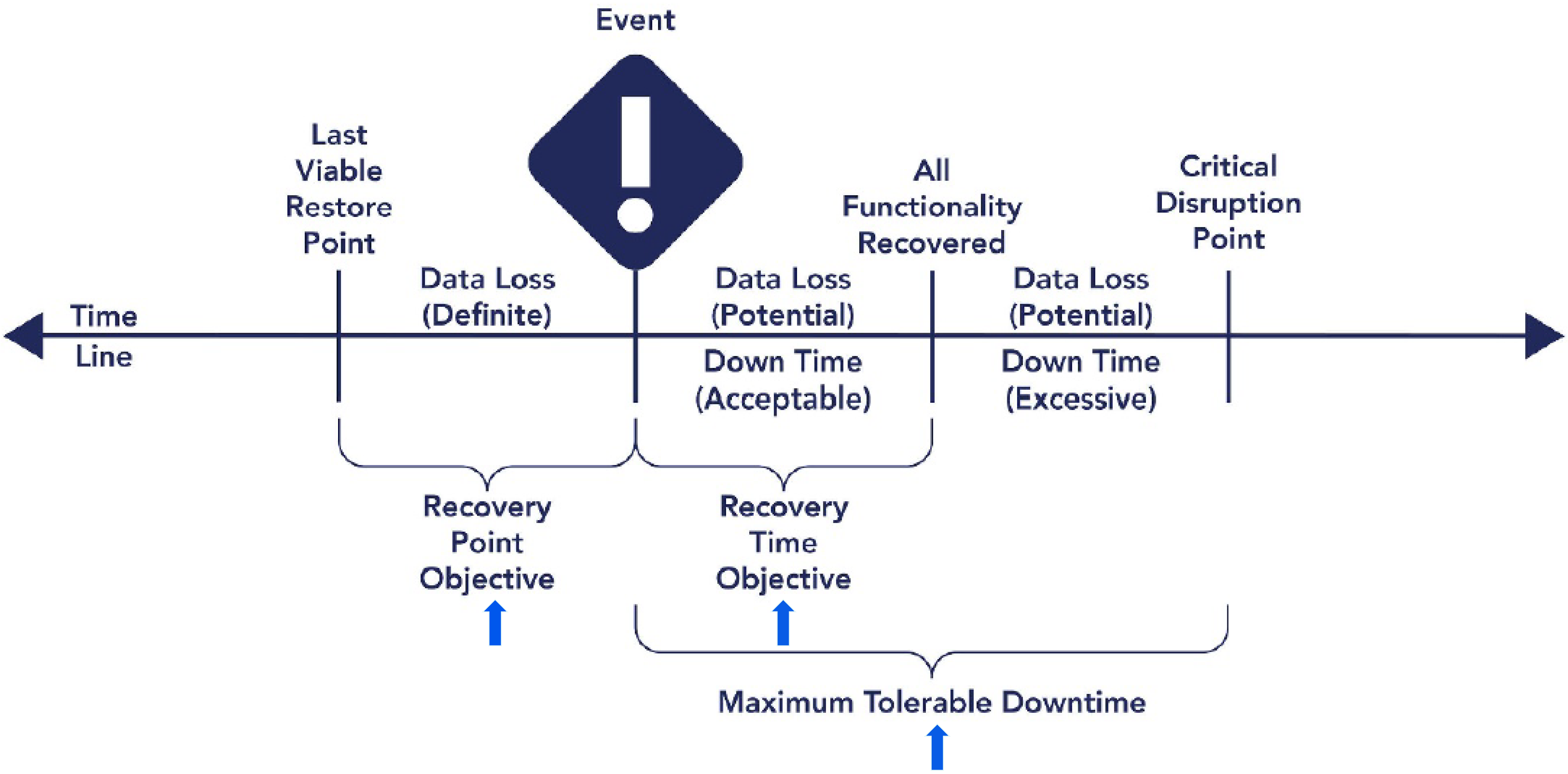
Airborne Demining in 3 Steps

Mapping

Detecting

Detonating

Impact of Disruption



FFIEC Information Technology Examination Handbook: Business Continuity Management, November 2019

Return Time Objective (RTO)

FFIEC

“Whether driven by customer expectations or technological advancement, previously established RTOs that were a few hours in duration may now require near real-time recovery. Therefore, it may be appropriate for management to reevaluate currently acceptable RTOs.”

What was good enough a few years ago, may not be good enough today.

FFIEC Information Technology Examination Handbook: Business Continuity Management, November 2019

Resilience

FFIEC

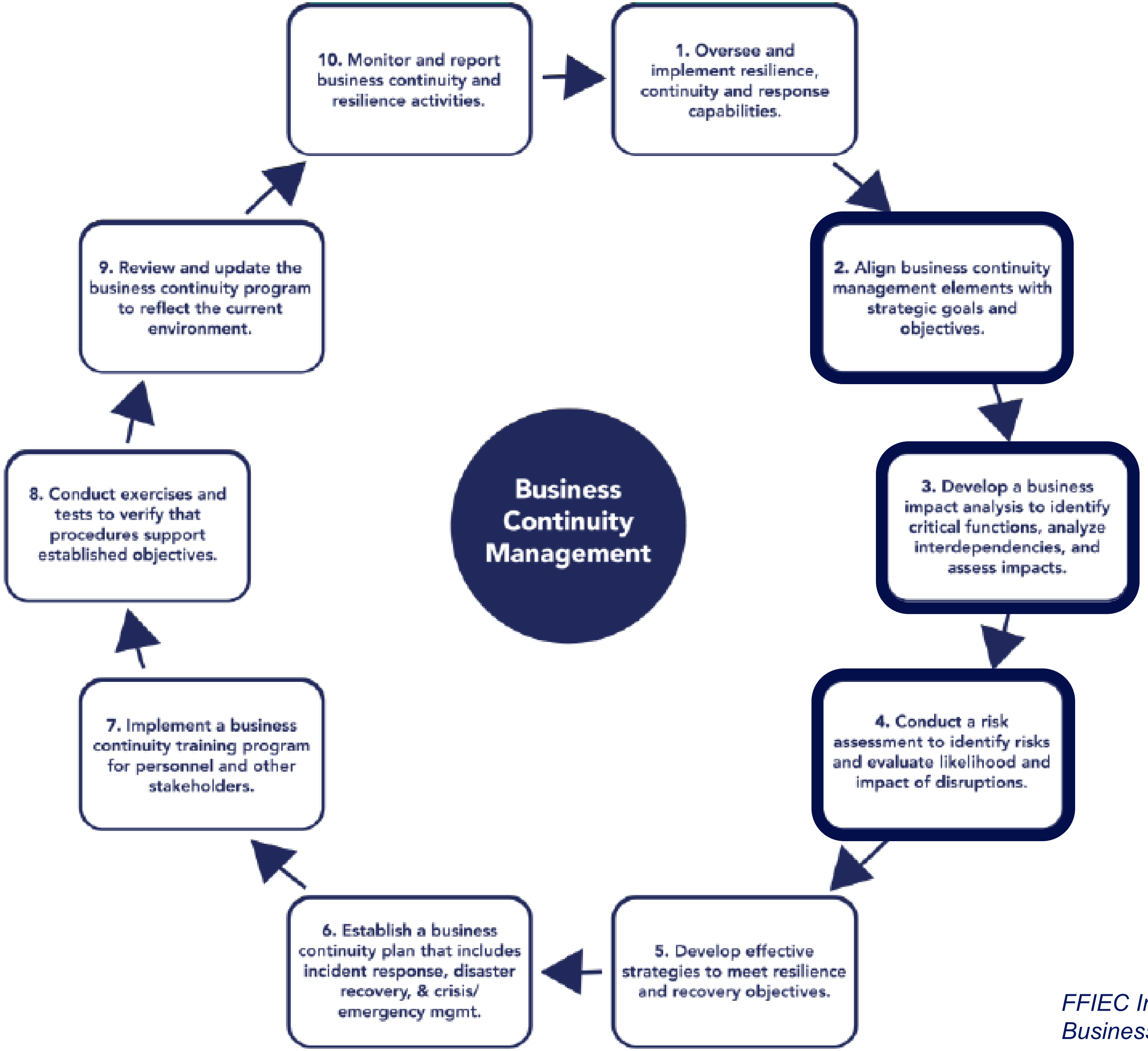
"The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."

FFIEC Information Technology Examination Handbook: Business Continuity Management, November 2019

Business Continuity Management (BCM)

- Compare inherent risk and effectiveness of risk mitigation against the entity’s risk appetite
- Verify whether test plans achieve stated objectives
- Monitor BCM testing to verify that issues (e.g. deviation from test plans and failed objectives) are appropriately identified and escalated

FFIEC Information Technology Examination Handbook: Business Continuity Management, November 2019



Business Continuity Management

1. Oversee and implement resilience, continuity and response capabilities.

2. Align business continuity management elements with strategic goals and objectives.

3. Develop a business impact analysis to identify critical functions, analyze interdependencies, and assess impacts.

4. Conduct a risk assessment to identify risks and evaluate likelihood and impact of disruptions.

5. Develop effective strategies to meet resilience and recovery objectives.

6. Establish a business continuity plan that includes incident response, disaster recovery, & crisis/ emergency mgmt.

7. Implement a business continuity training program for personnel and other stakeholders.

8. Conduct exercises and tests to verify that procedures support established objectives.

9. Review and update the business continuity program to reflect the current environment.

10. Monitor and report business continuity and resilience activities.

Strategic Alignment

Business Impact Analysis (BIA)

Risk Assessment

FFIEC Information Technology Examination Handbook: Business Continuity Management, November 2019

Business Impact Analysis (BIA)

- Identify critical business functions
- Identify interdependencies across business units
- Identify and analyze disruptive events

FFIEC Information Technology Examination Handbook: Business Continuity Management, November 2019

What Are Your "Crown Jewels"?

- Consider customer impact and regulatory expectations
- Ensure you can continue to serve your customers
- Consider customer impact and determine whether BCM solutions meet or exceed recovery objectives

FFIEC Information Technology Examination Handbook: Business Continuity Management, November 2019

BIA – Avoid "A Few Good Men" Management

- Candid conversations – focus on the current state
- Would you be able to achieve your recovery objectives?
- Allows management to identify and analyze gaps in critical processes that would prevent the entity from meeting its business requirements

BIA – Interdependency Analysis

- Identify single points of failure
  - Telecommunications or power
  - Network connections between branches
  - Data centers in close geographic proximity
  - Backups corrupted
  - Personnel
- Internal and Third-Party Services

FFIEC Information Technology Examination Handbook: Business Continuity Management, November 2019

Do You Know Your Cost of Downtime?

Other Expenses

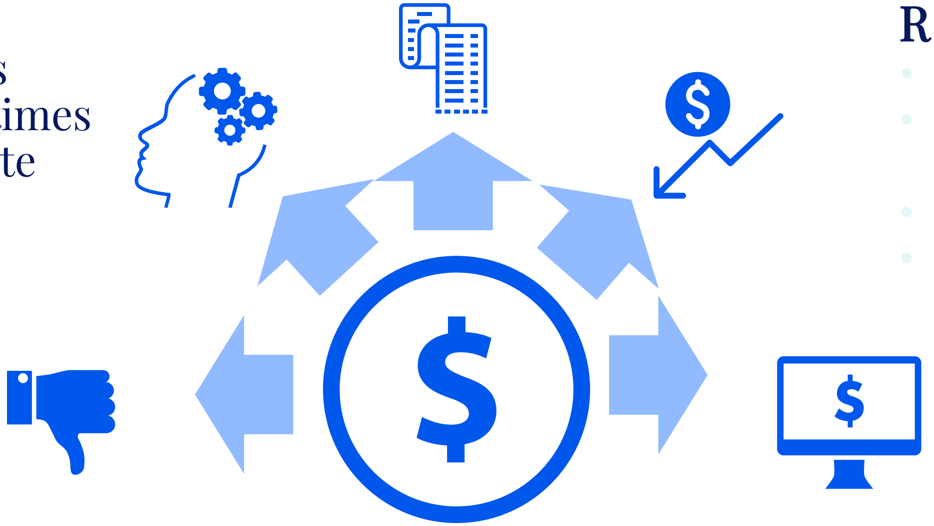
Temporary Employees, Equipment rental, overtime costs, extra shipping costs, travel expenses, legal obligations

Productivity

- Number of employees affected X hours out times X burdened hourly rate

Revenue

- Direct Loss
- Compensatory Payments
- Lost Future Revenue
- Billing Losses



Damaged Reputation

- Customers
- Suppliers
- Financial Markets
- Banks
- Business Partners

Financial Performance

- Revenue Recognition
- Cash Flow
- Lost Discounts (A/P)
- Payment Guarantees
- Stock Price

Know your downtime costs per hour, day, week, etc.

Downtime estimates range from $10,000 to $200,000 per hour of lost revenue

Landmines – Data

- Understand where data resides
  - Complex Environment
  - Cloud exposure
- Data Protection
  - Encrypted in transit and at rest
- Data Backup Strategy
  - Backup Frequency
  - Retention
  - Recovery Time and Costs
- Testing Frequency

Landmines

- Integration
  - Understand limitations with “backup in a box”
  - Understand how will communicate
- Lack of Testing and Validation
- Inadequate backups
- Inadequate security controls
- Failure to prioritize data
- Business need should drive strategy not technology
  - DR is a business issue, not just an IT issue

Landmines

- Throughput
  - Backups usually are incremental
  - Restores may be small amount of data localized to a single user or large amount for the full enterprise
- Insufficient Retention Periods
- SaaS applications

O365

Most SaaS providers follow a Shared Responsibility Model

Cloud Service Provider

Responsible for infrastructure and underlying services of SaaS applications

O365 does not include backup and recovery

Only 13% of businesses understand that data protection is solely on them

Customer Role

Responsible for data protection, including data entering, living in, and leaving the system

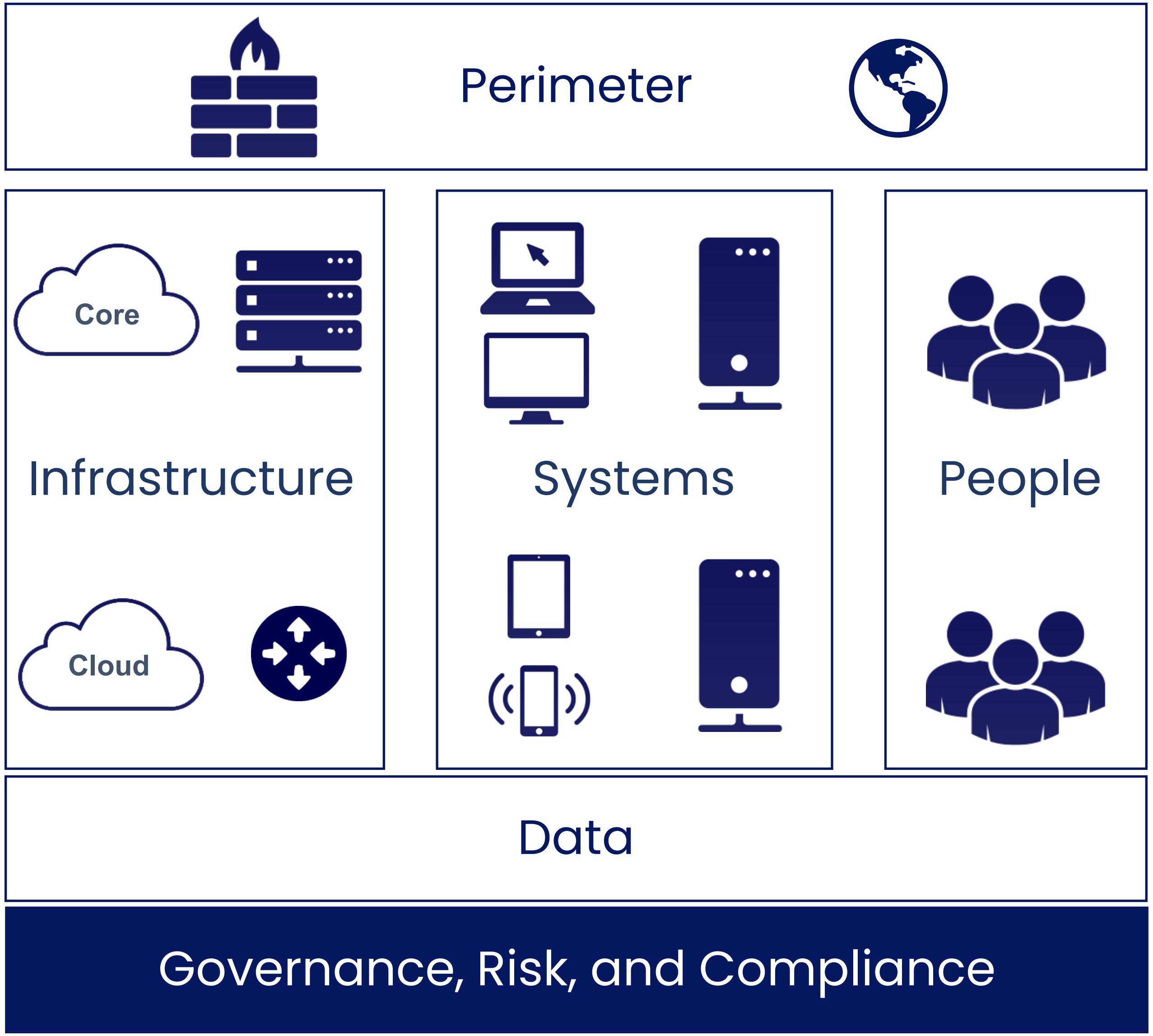
https://www.techtarget.com/searchdatabackup/feature/Data-protection-experts-weigh-in-on-SaaS-backup-confusion

FFIEC

> *“Security breaches involving cloud computing services highlight the importance of sound security controls and management’s understanding of the* ***shared responsibilities between cloud service providers and their financial institution clients.****”*

Joint Statement on Risk Mgmt. for Cloud Computing Services
https://www.ffiec.gov/press/pr043020.htm

Think Holistically



Perimeter

Infrastructure

Systems

People

Data

Governance, Risk, and Compliance

More Than Technology

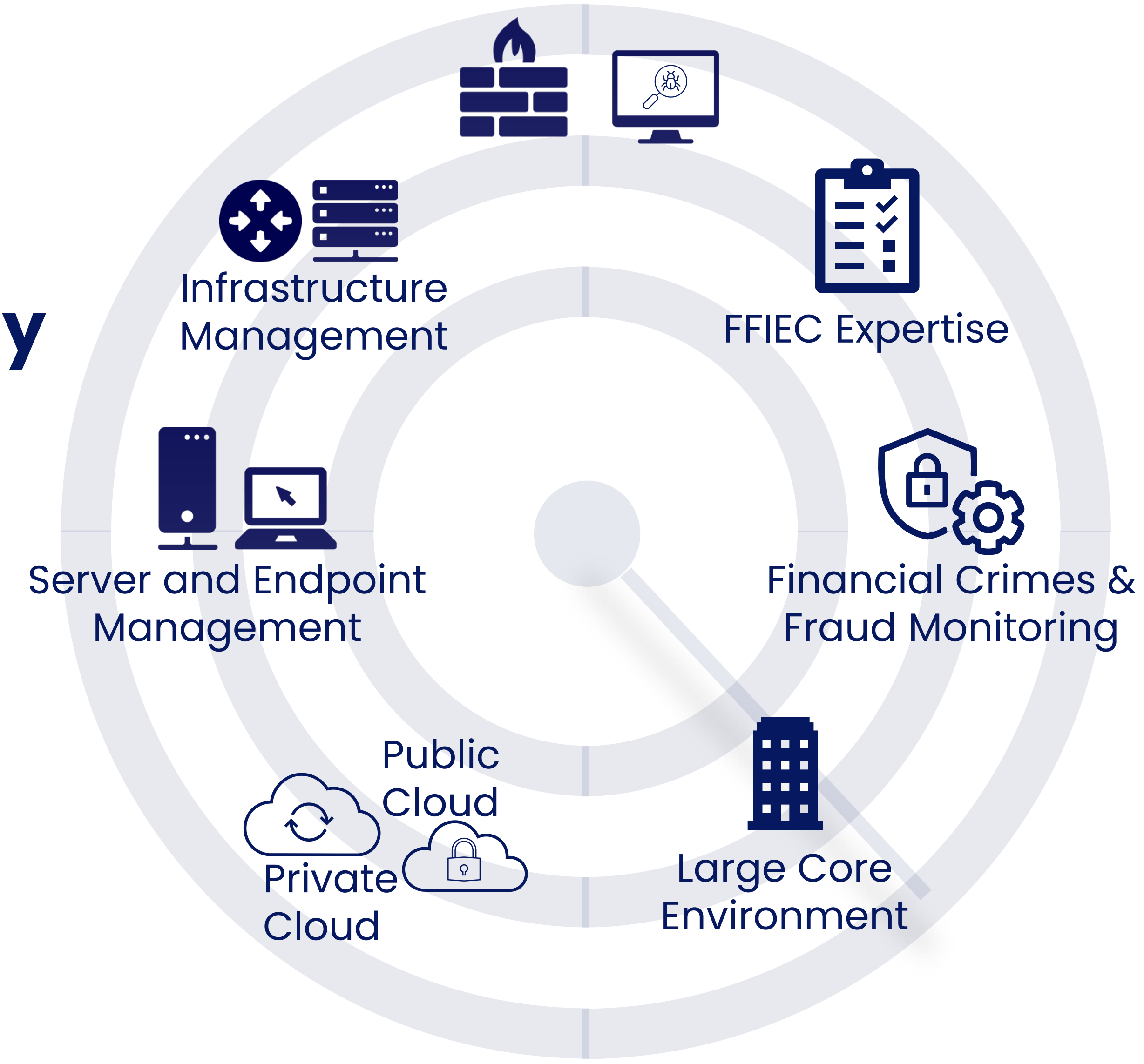
Gladiator Total Protect™

Comprehensive Information Security
built for Financial Institutions

Broad Expertise and Visibility

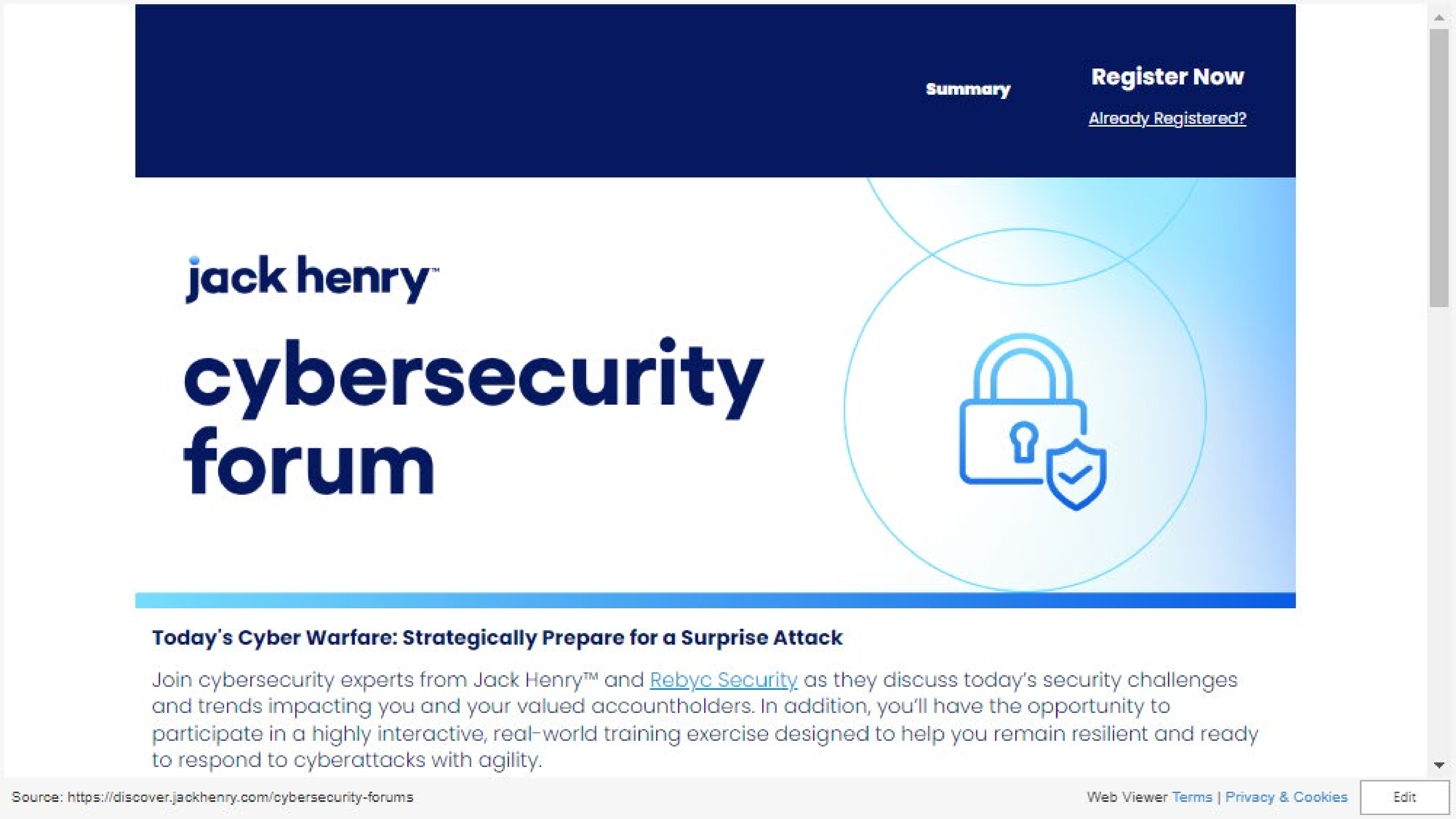
Jack Henry’s expertise and visibility is unmatched

Critical for accuracy and incident response support


Infrastructure Management
FFIEC Expertise
Server and Endpoint Management
Financial Crimes & Fraud Monitoring
Public Cloud
Private Cloud
Large Core Environment

Our Resume

- 25 Years of IT & InfoSec Services for FIs
- 250+ Certified Professionals
- Over 1,200 Clients
- Core Processor Agnostic
- Host/Maintain over 5,000 Servers
- Host/Maintain over 23,000 Endpoints



cybersecurity forum

Today's Cyber Warfare: Strategically Prepare for a Surprise Attack

Join cybersecurity experts from Jack Henry™ and Rebyc Security as they discuss today's security challenges and trends impacting you and your valued accountholders. In addition, you'll have the opportunity to participate in a highly interactive, real-world training exercise designed to help you remain resilient and ready to respond to cyberattacks with agility.

Source: https://discover.jackhenry.com/cybersecurity-forums

Jack Henry Cybersecurity Forums

Thursday, April 13	Kansas City Airport Marriott
Thursday, May 4	Sheraton Music City Nashville Airport
Thursday, May 25	Renaissance Chicago O'Hare Suites

https://discover.jackhenry.com/cybersecurity-forums jack henry™