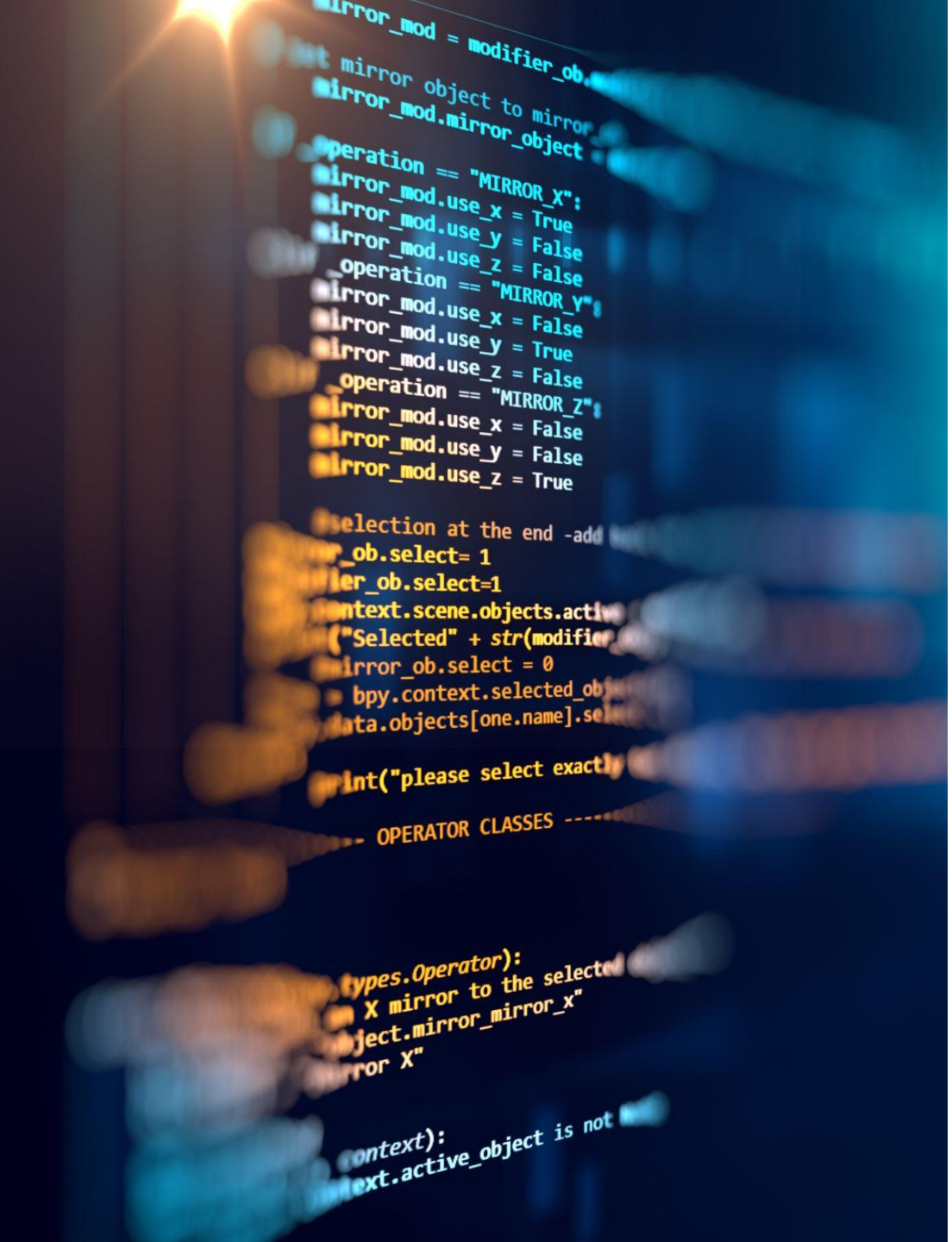
Cybersecurity Readiness

Aligning with Regulatory Expectations and Industry Standards

RCG RISK COMPLIANCE GROUP

DFW FPA Chapter Meeting
September 13, 2023



Cybersecurity Challenges

- **MORE** data in more places and easier accessibility.
- **MORE** devices and apps of variety connected.
- **MORE** technology solutions and software being rapidly deployed.
- **MORE** sophisticated cyber threats with greater chances of human error.

results in **MORE** data privacy risk.

Cybersecurity Threat Landscape

Cyber Attacks- More Difficult to Detect

- Attackers are staying dormant within a network upwards of 180 days before detection.
- Cyber attacks are more sophisticated using a combination of phishing and hacking techniques. IT, mobile devices and cloud service providers are key targets for attacks.

New Targets- Smaller Organizations

- There is a significant increase in cyber attacks targeting smaller organizations.
- Only a small percentage of small to medium-sized businesses are using threat monitoring/alerting toolsets to prevent breaches.

RCG RISK COMPLIANCE GROUP

Cybersecurity Threat Landscape

Cyber Criminals

- The Dark Web continues to be used to sell and lease malware, ransomware, botnets and the tech support to amateur cyber hackers to effectively perpetrate massive cybercrimes.

Data Breaches

- Data breaches are primarily caused by poor internal security practices. There is a significant surge in class-action lawsuits against organizations who failed to protect their client's data.

RCG RISK COMPLIANCE GROUP

Important to Recognize

- Cyber threats and attacks are not going away. It is important to fully embrace a cybersecurity culture to protect your business and client's data.
- This is not just an IT or Compliance issue to fix. It is everyone's responsibility at the organization to safeguard the environment.
- Partial compliance is ineffective.

RCG RISK COMPLIANCE GROUP

Important to Recognize

- There is no ‘silver bullet’ technology to ensure compliance.
- It is critical to leverage expertise and managed service providers. Cyber attackers are evolving their tactics and tools, your strategy must dynamically adapt.
- The cybersecurity program needs to be managed, monitored, and tested year after year.

RCG RISK COMPLIANCE GROUP

New Regulatory Expectations

The SEC has issued proposed cybersecurity rules that are expected to be finalized later this year or early 2024.

RCG RISK COMPLIANCE GROUP

Cybersecurity Readiness

- The National Institute of Standards and Technology (NIST) is a widely adopted industry framework and is the basis for the SEC prescribed cybersecurity standards and guidance.

- Enhanced controls are also defined within the framework categories to further advance the cybersecurity efforts beyond just the baseline requirements.

RCG RISK COMPLIANCE GROUP

Cybersecurity Maturity

- An effective cybersecurity program begins with:

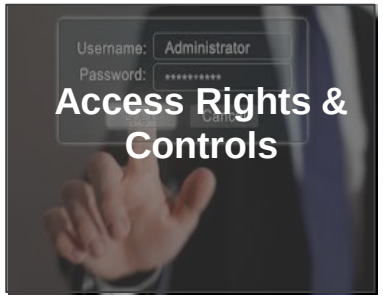
1. Understanding what cyber risks and threat types are relevant to your business operations.

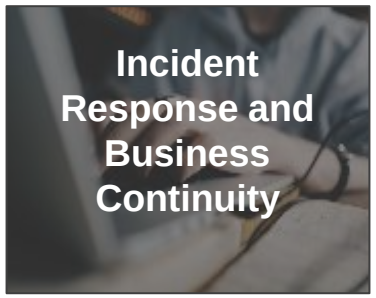
2. Assess the ‘maturity’ of current information security processes as aligned with industry standards. (i.e. NIST)

3. Identify any gaps, manage maintenance tasks, and track compliance.

RCG RISK COMPLIANCE GROUP

Cybersecurity Framework Categories





RISK COMPLIANCE GROUP

Cybersecurity Preparedness

Cyber Category	Security Controls
Governance & Risk Assessment	Governance-Oversight
	Assigned Responsibilities
	Information Security Policies & Procedures
	Risk Management/Assessment/Audit Program
Network Security	Threat Intelligence, Monitoring, & Network Management
	Vulnerability Scans
	Penetration Testing
	Malware Defense & Patch Management
	Remote Access Controls/Multifactor Authentication
	Audit Logging & Monitoring
Access Rights & Controls	Access Administration & Review
	Authentication & Password Controls
Data Loss Prevention	Asset Management, Data Inventory & Data Classification
	Data Retention & Destruction
	End point Device/Mobile Security- Encryption
	Data Transmission Security-Encryption
	Physical Security
	Validation of Client Identity
Vendor Risk Management	Due Diligence/Vendor Risk Assessment
Incident Response and Business Continuity	Cyber Incident Response Plan & Breach Handling Procedures
	Cyber Insurance
	Business Continuity Plan
	IT Disaster Recovery Backups/Testing
	Tabletop Exercises
Training & Awareness	Training & Awareness

Areas of Strength we see with Cybersecurity Programs:

- Cybersecurity assigned roles and responsibilities.
- Written information security policies. (basic)
- Anti-virus and patch management of critical updates are performed on firm assets.
- Encryption for emailing/sharing privacy data.
- Password controls and two factor authentication.
- Procedures to verify client identity.
- Physical security.
- Cybersecurity awareness- staff meetings/reminders.
- Business continuity planning- general response and recovery procedures.
- Email security appliance/archiving.

Cybersecurity Program Recommendations

1. Review & Update Policies.

- Ensure policies are comprehensive. Each of the control categories should be referenced with sufficient protocols to guide the employees and set expectations.
- Review with employees/acknowledgement. acknowledgement.
- Adhere to the policies and conduct periodic reviews for compliance.

2. Vulnerability assessments. Conduct vulnerability scans and penetration testing. The SEC stresses the importance of such tests as part of threat monitoring/ protection.

3. Risk assessment. Perform a cyber risk analysis that includes identifying cyber threat types, assign risk ratings, and verify mitigating controls.

RCG RISK COMPLIANCE GROUP

Cybersecurity Program Recommendations

4. User access reviews. Conduct user lists and assigned rights in all systems containing sensitive data. at least quarterly and document evidence.

5. Data inventory. Prepare a mapping to identify where privacy data resides and ensure appropriate safeguards are in place.

6. Vendor assessments. Conduct an annual vendor review. Capture evidence of controls including SOC reports and questionnaire responses to confirm they have acceptable cybersecurity controls in place.

7. Cyber Incident Response Plan. Create a cyber incident response plan that defines the protocols to respond, contain, recover, and handle post-incident steps.

RCG RISK COMPLIANCE GROUP

Cybersecurity Program Recommendations

8. Cybersecurity Business Continuity Plan. Ensure the plan is actionable to address both response and recovery strategies to mitigate significant business disruptions.

9. Security Event Log Retention. Work with IT to assess security event log history (i.e. firewall, operating system, email). Retention should be at least 6+months which is critical for forensic investigations of cybersecurity incidents to determine if a data breach.

10. Conduct Executive & IT Review Sessions. Conduct review sessions with IT and senior management regarding the status of the firm's cybersecurity program.

RCG RISK COMPLIANCE GROUP

Cybersecurity Program Recommendations

11. IT Disaster Recovery Testing. Conduct a ‘restore’ of your data being backed up. Do not rely just on backup indicators that files, systems, and network configurations can be recovered without issue.

12. Cybersecurity Training & Phishing Exercises. Formalize annual cybersecurity training and phishing exercises for employees. This includes new hire and remedial training.

13. Tabletop Exercise. Have an annual tabletop exercise facilitated to review incident scenarios and step through appropriate actions and best practices.

RCG RISK COMPLIANCE GROUP

Cyber incident preparedness

Why are tabletop exercises important?

- Review and rehearse incident response procedures.
- Understand roles and responsibilities.
- Discuss best practices and strategies.
- Identify any weaknesses, gaps and take-aways.

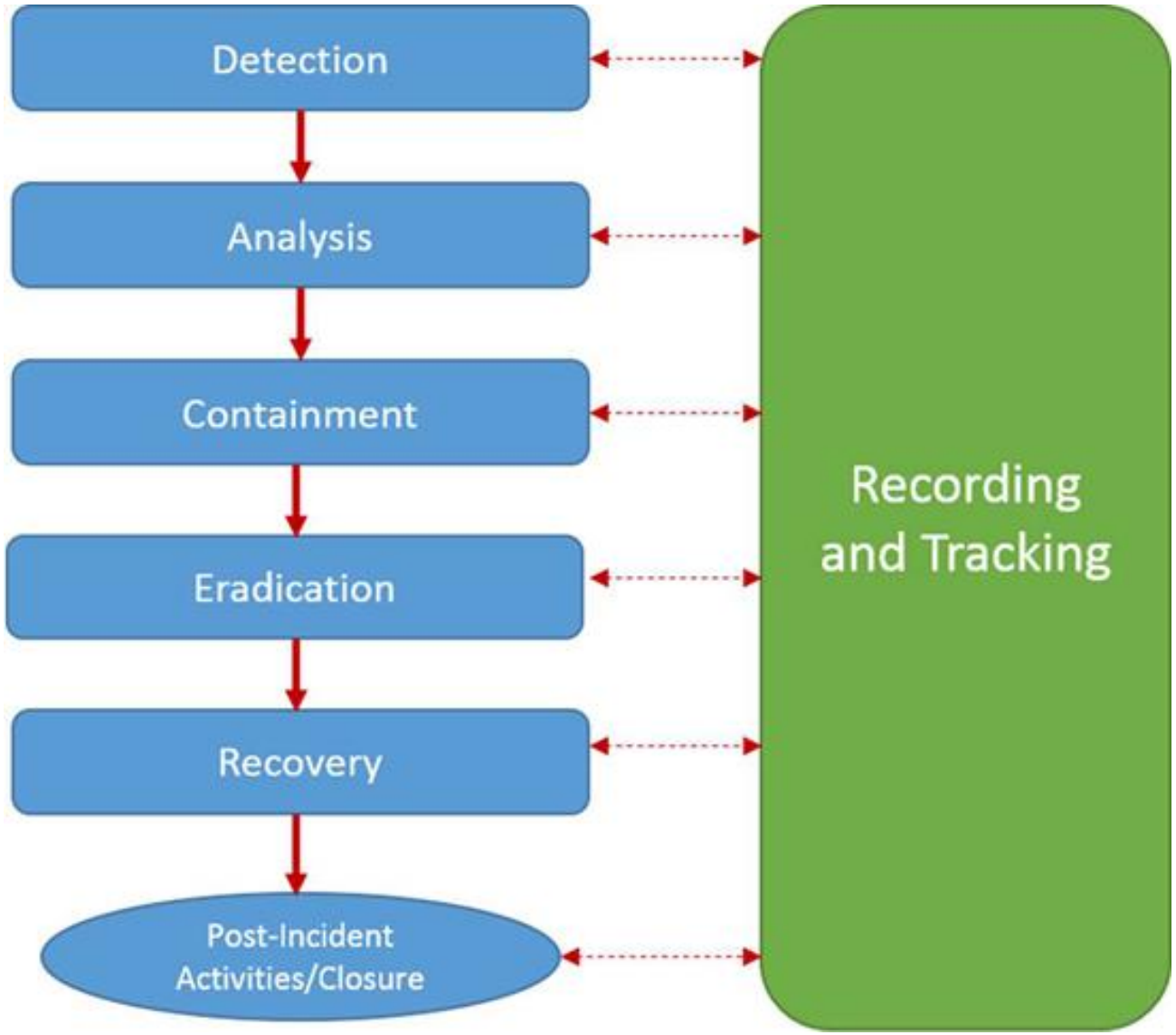
RCG RISK COMPLIANCE GROUP

Cyber Incident Response Planning

Immediate Response
- Detection
- Immediate Mitigation
- Escalate

Continuing Response
- Analysis
- Containment
- Eradication
- Recovery

Post Incident
- Investigation
- Compliance & Notification
- Reporting
- Post Incident Remediation/Lessons Learned/Training



Cybersecurity Incident Response "Playbook"

Step 1: Preparation- Identifying Your Team

Incident Response Team:

- Incident Manager
- IT Infrastructure/Systems/Information Security
- Compliance Officer
- Executive Leadership
- General Counsel- Focus Legal Team
- Communications

External Support Providers:

- Cyber Insurer
- Forensic Resources/Cybersecurity Specialists
- Outside Data Privacy Counsel
- Public Relations
- Software Vendors/Business Service Partners

RCG RISK COMPLIANCE GROUP

19

Cybersecurity Incident Response "Playbook"

Step 2: Detection & Identification

- Look for suspicious activity/alerts triggered with detection tools in place.
  - Perimeter controls (Firewalls, VPN, IDS/IPS)
  - Endpoint monitoring (Laptop, Desktop, Mobile, Server)
  - Security event logs
  - External threat intelligence

- What happened to cause the alert? (Malware, failed hardware/ software, phishing attack, hacker, etc.)

- What data was compromised? (PII, financial, operations/intellectual property)

- Could its disclosure cause potential harm to a person or company?

Cybersecurity Incident Response "Playbook"

Step 3: Containment

- What controls do you have in place to stop the spread of the incident?

Step 4: Eradication

- Remove malware or rebuild systems
- Remove back doors, delete accounts, change passwords, etc.

Cybersecurity Incident Response "Playbook"

Step 5: Recovery

- Harden systems
- Implement new controls
- Bring systems back online

Step 6: Post Incident/Review

- Record and track incident handling actions.
- Breach notification- if required
- Compliance/regulatory reporting
- Update policies and procedures
- Lessons learned/training

RCG RISK COMPLIANCE GROUP

Closing Comments

Thank you for your participation!

Mark Madar
National Practice Leader
Risk Compliance Group, LLC

Phone: 330-701-1308
Email: mmadar@riskcompliancegroup.com

www.riskcompliancegroup.com

RISK COMPLIANCE GROUP