CYBER SECURITY FROM THE GROUND UP

Building Cyber Resilience

Adam Evans
VP, Cyber Operations and
Chief Information Security Officer

September 12, 2019

TODAY'S TOPICS

DEFEND

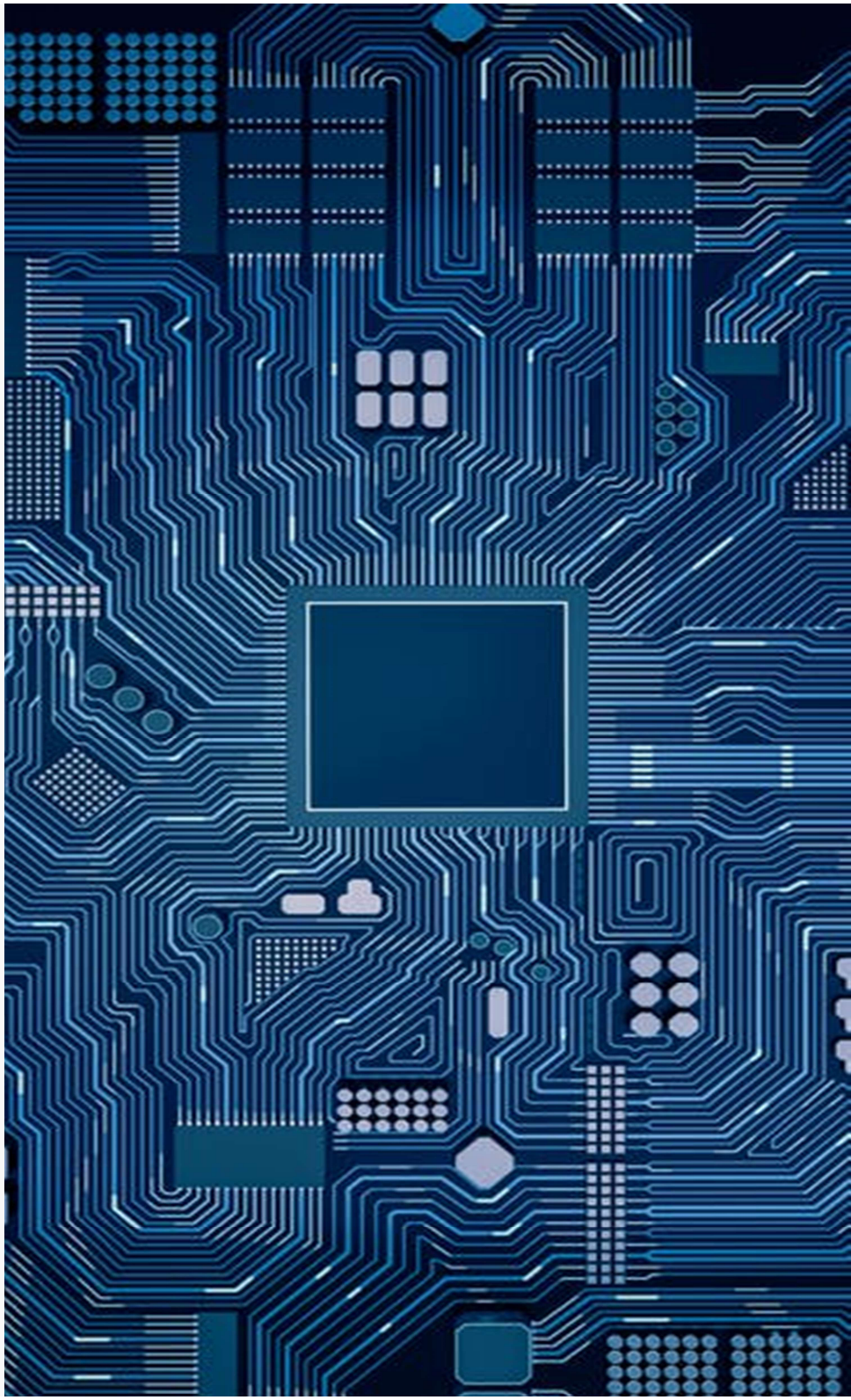
- Ensuring effective security and monitoring technology is in place to protect your organization against cyber attacks

COMMUNICATE

- Why education and awareness are critical to protecting the confidentiality and integrity of your organization's information

PREPARE

- Planning and executing cyber ranges to prepare your organization for a cyber event



GINNI ROMETTY, IBM CEO

"Cyber crime is the greatest threat to every company in the world."

DAVE MACKAY, RBC CEO

"As we build the digitally-enabled relationship bank, we're tying together operations, services and frontline systems in an integrated world, which offers ease and convenience for our clients, but unfortunately could also make us vulnerable to cyberattacks.

So we have to continue to protect the system with a layered approach to security and remain vigilant by staying aware and being cautious."

AREAS TO CONSIDER

KEY CYBER CHALLENGES

Commoditized Threat Landscape

Third Party Risk

Digital Innovation

Regulatory Risk

Talent Gap

Defend

DEFEND

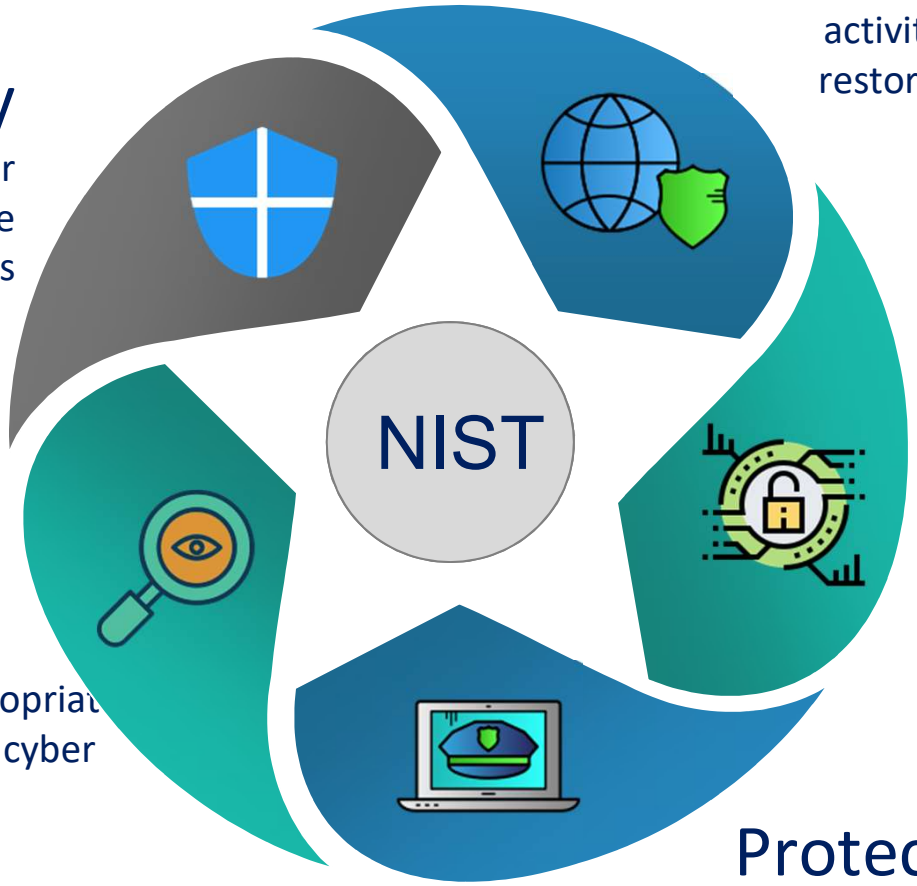
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CYBER FRAMEWORK

Recover

Implement appropriate activities for resilience and restoring services impaired due to a cyber event

Identify

Understand your organization to manage cyber risks



Respond

Implement appropriate activities to take action on a detected cyber event

Detect

Implement the appropriat activities to identify cyber events

Protect

Implement safeguards to ensure delivery of critical services

DEFEND

A MODERN CYBER STRATEGY

Cross-functional Responsibility
An integrated, cross-functional security operating model is essential, underpinned by a supporting data model.

Talent & Culture
Build a top talent strategy and create a strong risk and security culture, starting from tone at the top.
.

Risk Management
Develop a comprehensive assessment and testing program that provides control assurance, granular risk identification, and actionable reporting.

External Partnerships
External partnerships are required to build and mature capabilities.

Industry-leading Cyber Capabilities
Aligned to the NIST Cyber Security Framework. Embed Security as a Service into the technology fabric.

Expected outcomes for a new modern strategy are:

- Faster response time
- Greater resiliency
- Reduced risk
- Increased business alignment
- Continuous assurance
- Centralized monitoring
- Improved efficiency and ROI
- Enhanced regulatory compliance
- Contractual commitments

POLL

Does your organization currently have a cyber strategy in place?

a) Yes

b) No

c) We're working on it.

Communicate

COMMUNICATE

CYBER RISKS TO BUSINESS

- Loss of customer, client or employee information
- Loss of corporate information
- Loss of technology information
- Internal fraud or loss
- Electronic channel fraud
- External-facing service disruption (DDoS)
- Internal function disruption
- Data corruption/modification
- Third party/supply chain threats

COMMUNICATE

EMPLOYEES PLAY A CRITICAL ROLE

Employees are key to prevention and protection. Education and awareness is critical so that employees know what they can do to prevent malicious activity.

TRAIN AND TEST

Assign and track training resources and phishing simulations based on employee needs.

MEASURE

Benchmark the effectiveness of cybersecurity awareness training.

ENGAGE

Engage employees with gamification via personal and departmental risk scores, e.g. cyber dashboard

POLL

According to Wombat's 2018 State of the Phish survey, 76 percent of organizations say they experienced phishing attacks in 2017. Does your organization currently run regular phishing simulations for your employees?

a) Yes

b) No

COMMUNICATE

RESOURCES FOR CLIENTS

Clients also play a critical role in cybersecurity. Education and awareness through websites and marketing materials provides important information for clients on how to protect themselves online.

RBC.COM/CYBER

MENU Cyber Security

Be Cyber Aware

In today's digitally connected world, not everyone is who they claim to be. That's why we are committed to helping our clients learn how to protect themselves and their data.

Scam Alerts

Visit our Scam Alerts page to stay informed on the latest cyber scams affecting RBC clients.

Prepare

PREPARE

BOOSTING RESILIENCE WITH CYBER RANGES

Cyber and risk management leaders should consider the different use cases for a cyber range. Organizations can foster new skills and competencies to increase organizational resilience and manage the new risks of digital business. By 2022, 15% of large enterprises will be using cyber ranges to develop the skills of their security teams, up from 1% today. – Gartner May 2018

- ✓ Strengthen cyber crisis response capabilities
- ✓ Apply playbook practices
- ✓ Reinforce roles and responsibilities related to cyber crisis response
- ✓ Deepen understanding of relevant issues related to a cyber scenario to improve preparedness
- ✓ Reinforce escalation protocols and decision-making accountabilities

WHO SHOULD YOU CALL?

- Do you have an Incident Response retainer?
- Do you have the number to call?
- Who can activate the retainer?
- What services do they supply?
- What if they are busy?
- Do you have a backup plan?
- Do they conduct proactive and reactive services?

PREPARE

PEOPLE, PROCESSES AND TECHNOLOGY

- Who are your key people to bring systems online?
- Do you have a generalist who understands how everything works?

- What key processes are required?
- What are the dependencies for those processes?

- What key technologies do you rely on?
- How quickly can you deploy new technology if needed?

CYBER RANGE PROVIDERS

Defend.
Communicate.
Prepare.

THANK YOU

Visit RBC.COM/CYBER to learn more.