NORTH RISK PARTNERS®

XIGENT
Result Driven IT

# PROTECT YOUR BUSINESS IN THE DIGITAL AGE WITH A CYBER SECURITY PROGRAM

JUNE 2024

# PRESENTER

## Amos Aesoph

Chief Information Security Officer

Xigent



NORTH RISK PARTNERS®

XIGENT Result Driven IT

# INTRODUCTION & AGENDA

- The Evolving Threat Landscape
- Why Information Security Matters
- Core Components of an Information Security Program
- The Role of Insurance in Information Security
- Case Study: UnitedHealth
- Implementing an Information Security Program
- The Role of Leadership in Security
- Overcoming Common Security Challenges



NORTH RISK PARTNERS®

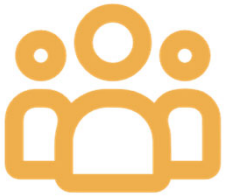
XIGENT
Result Driven IT

# THE EVOLVING THREAT LANDSCAPE

- Malware, Phishing, Ransomware
- Rising frequency of attacks
- Increasing cost of data breaches
- $4M average cost of a breach
- Sector-specific vulnerabilities
- Equifax Data Breach
- WannaCry Ransomware Attack
- SolarWinds Supply Chain Attack

# WHY INFORMATION SECURITY MATTERS

Protection of Sensitive Data



Customer Trust & Brand Reputation

Regulations & Compliance

Financial Implications of Data Breaches

# CORE COMPONENTS OF AN INFORMATION SECURITY PROGRAM

**Information Security Program**

### Risk Assessment

- Identifying assets, threats, & vulnerabilities
- Evaluating potential impact & likelihood

### Policy Development

- Creating security policies & procedures
- Importance of employee awareness & training

### Implementation of Security Controls

- Technical controls (firewalls, encryption, anti-virus)
- Admin controls (access controls, incident response plans)
- Physical controls (security badges, surveillance)

### Monitoring & Response

- Continuous monitoring for suspicious activities
- Incident response & management
- Regular security audits & updates

# THE ROLE OF INSURANCE IN INFORMATION SECURITY

## Cyber Insurance as a Safety Net

- Financial Protection
- Risk Management
- Recovery Support

## Coverage Options & What they Include

- Data Breach Costs
- Business Interruption
- Third-Party Liability

## The Process of Filing a Claim

- Initial Notification
- Documentation & Investigation
- Claim Resolution & Payout

# CASE STUDY: UNITEDHEALTH OVERVIEW

- Date: Discovered in February 2024
- Scope: The breach compromised the personal and health information of millions of individuals across the United States.
- Data Compromised:
  - Personally identifiable information (PII)
  - Protected health information (PHI)
  - Approximately 4TB of data
  - Names, Social Security numbers, birth dates, addresses, and health data.

**UnitedHealth data breach caused by lack of multifactor authentication, CEO says**

United Healthcare

# CASE STUDY: UNITEDHEALTH - IMPACT

- Financial Impact:
  - Immediate expenses reaching $872 million
  - Total costs estimated to grow to $1.6 billion
  - UnitedHealth paid a ransom of $22 million
- Reputation Damage:
  - Loss of trust among customers and stakeholders,
  - Extensive efforts to restore confidence and reassure affected individuals
- Operational Disruptions:
  - Major disruptions across U.S. healthcare systems,
  - Impacts on pharmacy and medical claims services
  - Replacement thousands of laptops, rebuild its data center network, and add capacity

**UnitedHealth Paid Hackers $22 Million, Fixes Will Soon Cost Billions**

# CASE STUDY: UNITEDHEALTH RESPONSE

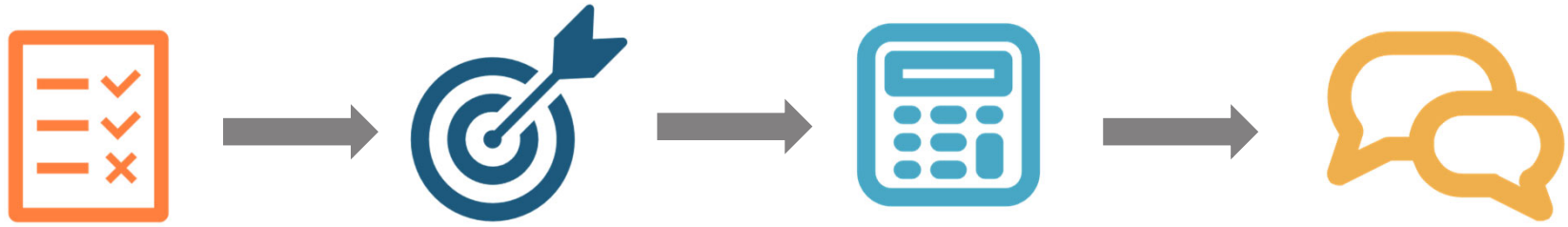
- Incident Response:
  - Engaged cybersecurity
  - Support from Google, Microsoft, and Amazon
- Regulatory Compliance: ongoing communication with law enforcement and regulatory bodies, providing appropriate notifications and cooperating with investigations.
- Security Enhancements:
  - Multi-factor authentication
  - Enhanced security protocols.
  - Support policy changes for mandatory minimum security standards

**UnitedHealthcare CEO says 'maybe a third' of US citizens were affected by recent hack**

# CASE STUDY: UNITEDHEALTH – LESSONS LEARNED

- The necessity of continuous monitoring and updating of security measures to address evolving threats.
- The importance of having a well-defined incident response plan to mitigate the impact of breaches.
- The need for regular employee training to foster a culture of security awareness.

# IMPLEMENTING AN INFORMATION SECURITY PROGRAM



Assess Current Security Posture

Develop a Strategic Plan with Goals & Timelines

Allocate Resources & Budget

Engage Stakeholders & get Executive Buy-in

# THE ROLE OF LEADERSHIP

**Foster a Security-First Mindset**

- Setting the tone, allocating resources, establishing policies

**Ensuring Continuous Improvement & Adaptation to New Threats**

- Regular Security Assessments, staying informed on emerging threats, implementing adaptive security measures

**Implementing Regular Training & Updates**

- Employee Awareness Programs, skill development, policy & procedure updates

# OVERCOMING COMMON CHALLENGES

**Budget Constraints & Cost Justification**

- Identifying Cost-Effective Solutions
- Demonstrating ROI on Security Investments
- Prioritizing Critical Security Measures

**Balancing Security with Business Operations**

- Integrating Security into Business Processes
- Minimizing Operational Disruptions
- Encouraging a Collaborative Approach

**Keeping up with Evolving Threats & Technology**

- Continuous Monitoring & Threat Intelligence
- Regular Technology Upgrades
- Adopting a Proactive Security Stance

**Engaging & Training Employees**

- Security Awareness Training
- Promoting a Security-First Culture
- Providing Ongoing Education & Support

# QUESTIONS & DISCUSSION

# CONCLUSION & RECAP