Risks Lurking in the Shadows of Digital Transformation

Preparing to Manage New Digital Risks
Agenda

• Implications of Digital Transformation = Digital Risk
• The Emergence of Digital Risk Management
• Implementing an Integrated Approach to Digital Risk Management
• Getting Started: Assess Elements of Digital Transformation & Digital Risk
• Q&A
DIGITAL TRANSFORMATION

Activate & Monetize

Operational Efficiency

Data

New Customer Experiences

New Product Development
In a 2016 study of non-IT executives, 71% said that concerns over cybersecurity are impeding innovation in their organizations.
– Gartner

By 2020, 60% of digital businesses will suffer major service failures, due to the inability of IT security teams to manage digital risk.
– Gartner

73% of respondents agreed that the relationship between IT security and business risk can be difficult to coordinate.
– ESG Custom Research, Cybersecurity and Business Risk Survey, March 2018

2018 study of CEO’s showed 62% have a management initiative or transformation program in place to make the business more digital.
– Gartner
MODERNIZATION
MODERNIZATION

Digital Business

Hackers & Malware

Phishing

IoT

Cloud

Vulnerabilities

Robotics

MALICE
MANDATES
SPEED OF CHANGE
COMPLEXITY OF BUSINESS
AMPLIFICATION
OF RISK
Digital Risk is the greatest facet of risk that businesses face…

![Digital Risk vs Traditional Business Risk Graph](image)
…that requires a **New Perspective**
MANAGE RISK & OPTIMIZE YOUR BUSINESS

IDENTIFY RISK
ASSESS RISK
TREAT RISK

MANAGE PROCESS AUTOMATION RISK
MITIGATE CYBER ATTACK RISK
MODERNIZE YOUR COMPLIANCE PROGRAM
MANAGE DYNAMIC WORKFORCE RISK
MANAGE THIRD PARTY RISK
SECURE YOUR CLOUD TRANSFORMATION
COORDINATE BUSINESS RESILIENCY
EVOLVE DATA GOVERNANCE & PRIVACY

INTEGRATED RISK MANAGEMENT
EVOLVED SIEM / ADVANCED THREAT DETECTION & RESPONSE
SECURE, RISK-BASED ACCESS & AUTHENTICATION
OMNI-CHANNEL FRAUD PREVENTION
ADVANCED RISK AND CYBERSECURITY SERVICES

RSA ARCHER SUITE
RSA NETWITNESS PLATFORM
RSA SECURID SUITE
RSA FRAUD & RISK INTELLIGENCE SUITE
RSA RISK & CYBER SECURITY PRACTICE

IT
SECURITY
RISK MANAGEMENT
Implementing an Integrated Approach to Digital Risk Management
An Integrated Approach To Digital Risk Management

** MANAGE DYNAMIC WORKFORCE RISK **

** MANAGE PROCESS AUTOMATION RISK **

** MITIGATE CYBER ATTACK RISK **

** MODERNIZE YOUR COMPLIANCE PROGRAM **

** SECURE THE JOURNEY TO THE CLOUD **

** COORDINATE BUSINESS RESILIENCY **

** EVOLVE DATA GOVERNANCE & PRIVACY **

** IDENTIFY RISK **

** ASSESS RISK **

** TREAT RISK **

Understand the strategic context of the risk

Establish teams & processes that connect operational events to business impacts

Leverage technology solutions to automate and optimize processes

Utilize capabilities to improve each domain by leveraging data and processes across your program
An Integrated Approach To Digital Risk Management

**IDENTIFY RISK**
- Understand the business impact of the attacks
- Leverage technical and business context to prioritize

**ASSESS RISK**
- Establish a security operations center (SOC) with defined procedures

**TREAT RISK**
- Leverage automation during responses to attacks
- Create visibility across the infrastructure to identify and escalate potential security alerts

**MANAGE PROCESS AUTOMATION RISK**

**MITIGATE CYBER ATTACK RISK**

**MODERNIZE YOUR COMPLIANCE PROGRAM**

**SECURE THE JOURNEY TO THE CLOUD**

**COORDINATE BUSINESS RESILIENCY**

**EVOLVE DATA GOVERNANCE & PRIVACY**
An Integrated Approach To Digital Risk Management

1. IDENTIFY RISK
2. ASSESS RISK
3. TREAT RISK

- MANAGE PROCESS AUTOMATION RISK
- MITIGATE CYBER ATTACK RISK
- MODERNIZE YOUR COMPLIANCE PROGRAM
- MANAGE DYNAMIC WORKFORCE RISK
- MANAGE THIRD PARTY RISK
- SECURE THE JOURNEY TO THE CLOUD
- COORDINATE BUSINESS RESILIENCY
- EVOLVE DATA GOVERNANCE & PRIVACY

SECURITY OPERATIONS
Digital Risk Maturity

OPTIMIZED
- Sharing and Collaborating Across Silos
- Integrated business/risk context
- Priorities and resources aligned with risk and business objectives

MANAGED
- Platform Approach
- Pervasive Visibility
- Leverage Technology
- Integrate Silos

SILOED
- Ad Hoc, Reactive
- Trigger Events
- Tactical POV
RSA Risk Frameworks

Assessing Digital Risk Maturity: Financial Services Company

Compliance Requirements:
19 US State PII Laws, GDPR, PCI, and FINRA Member

Lowest Common Denominator Capabilities (partial list):
- Security Plan, updated annually
- Annual Audit (PCI, Risk)
- Logging of event logs for 7 years
- Real-time Security Event Monitoring
- Vulnerability Scanning
- 72 hour Breach Notification

Maturity Quantification:
- Overall Score: 50.4 out of 100
- Focus Breakdown:
  - Pre-breach Planning: 5.7 out of 20
  - Operational Security: 11.4 out of 20
  - Dwell Time Reduction: 8.5 out of 20
  - Remediation: 19.1 out of 20
  - Post-incident Handling: 5.7 out of 20

Overall Breach Readiness:
Average 10.8 per category, Average range with 3 areas below average
## RSA Risk Frameworks

<table>
<thead>
<tr>
<th>MATURITY QUALIFICATION</th>
<th>Overall Score:</th>
<th>50.4 out of 100</th>
</tr>
</thead>
</table>

### Pre-Breach Preparedness
- **LEFT OF BREACH** (PRE-BREACH)
- **PREPAREDNESS**
  - Minimal cybersecurity awareness and poor preparation to respond to breach.

### Breach Risk Reduction (Breach Deflection)
- **BREACH RISK REDUCTION** (BREACH DEFLECTION)
  - Limited testing of enterprise breach risk tolerance (system specific) and limited follow-through to adapt to threats, process, IT and security operational issues to reduce risk of a breach and optimize Incident Response (IR) to reduce impact.

### Breach and Initial Incident Response
- **BREACH AND INITIAL INCIDENT RESPONSE**
  - Minimal ability to identify breaches with no ability to measure impact. Ad hoc response capabilities.

### Breach Remediation
- **BREACH REMEDIATION**
  - 19.1 out of 20
  - Operational effectiveness to understand impact and impacted systems and effectively remediate breaches with automated assistance from technology.

### Right of Breach (Post Breach) Adaptation
- **RIGHT OF BREACH** (POST BREACH)
  - No follow-up post breach to improve capabilities on pre-breach based on GAP and learnings from breach.

---

**Impact Analysis**

Prepare for Breach to Reduce Risk of Breach and Breach Impact

- **POST-INCIDENT HANDLING**
  - Lessons Learned and adapt to Reduce Risk

- **RECOVER**
  - RemEDIATE and Prevention

- **ERADICATE**
  - Dwell Time

- **ANALYZE**
  - Awareness

- **CONTAIN**
  - Dwell Time Reduction Actions

- **PREPARE**
  - Adapt and optimize operational IT and Security