Improve Security, Privacy and Compliance with Continuous Oversight

Fouad Khalil, VP Compliance, SecurityScorecard
The Landscape From Above
DATA BREACH STATISTICS
DATA RECORDS LOST OR STOLEN SINCE 2013
14,717,618,286
DATA RECORDS ARE LOST OR STOLEN AT THE FOLLOWING FREQUENCY
EVERY DAY
6,390,629
Records
EVERY HOUR
266,276
Records
EVERY MINUTE
4,438
Records
EVERY SECOND
74
Records
Data Breach Landscape

• External actors remain the primary cause of data breaches
• Hacking remains the primary cause of data breaches
• Denial of Service (SoS) is the most prevalent hacking incident
• Amplified Distributed Denial of Service (DDoS) attacks increased from 25% in 2013 to 75% of DDOS attacks in 2018
• Databases are the most often breached asset, closely followed by POS terminals and controllers

Verizon Data Breach Investigations Report
https://enterprise.verizon.com/resources/reports/dbir/
The Data Breach Cost Landscape

- Global per capita data breach costs increased from $141 in 2017 to $148 in 2018
- The Top Three Cost Savings Factors were incident response team, encryption use, and BCM involvement
- The Top Three Cost Additions were third-party vendors, extensive cloud migration, and compliance failures.
- New this year: AI platform security automation solutions saved $8/compromised record and extensive IoT use increased cost by $5/compromised record

Ponemon Cost of Data Breach Study
The Compliance Landscape

• Implementation of GDPR:
  • Statista.com indicated that in the UK Banks spent £66M and Technology and Communications companies spent £20B
• New York Department of Financial Services Cybersecurity Requirement
• California Consumer Privacy Act (CCPA) passed (America’s GDPR)
• NIST Cybersecurity Framework updated
• ISO 27000 updated
• COSO Framework updated
The Risk and Compliance Struggle is Invisibility
Identification: Invisible Risks

- Web Application Security
- Network Security
- Endpoint Security
- Patching Cadence
- DNS Health
- IP Reputation
Action Plan: Invisible Process

- Policy: Formal organizational goals
- Procedures: Designated responsible parties and daily duties
- Implementation: Settings, configurations, third-party vendors
- Measurement: Testing, baselines, key performance indicators
- Management: Detecting anomalies, responding to changes, governance
Budgets: Invisible money

- 69% of companies see compliance mandates driving spending.
- 88% companies spent more than $1 million on preparing for the GDPR.
- 25% of organizations have a standalone security department.

Supply Chain: Invisible threat

- SLAs only cover what third-party says, not what it does
- Fourth parties increase risk
- Correlated and uncorrelated risks
Life cycle: Invisible improvement

- Threats evolve throughout the life cycle. Risk is continuous process.
- Risk analysis
- Risk monitoring
- Risk response
- New risk assessment
Moving to a Mature Model
Risk Analysis: The First Step

- **Identify**
  - locations:
    - systems, networks, software and devices
    - store, transmit, process, and collect
  - Types of data
    - Public
    - Non-public personally identifiable

- **Assess**
  - Risk of unauthorized access
  - Impact

- **Analyze**
  - Likelihood $\times$ Impact/Cost

- **Set Tolerance**
  - accept
  - transfer
  - refuse
  - mitigate
Establish Controls: The Second Step

- **Systems and networks**
  - Assign roles and responsibilities
  - Assess control effectiveness
  - Create Incident Response Plan

- **Vendor risk management**
  - Set SLA metrics
  - Monitor controls

- **Social engineering**
  - Employee training
  - Anti-malware/ransomware
Compliance Alignment: The Third Step

- **Laws**
  - GDPR
    - Austrian entrepreneur: CCTV outside business led was fined 4800EU
    - German chat platform: data breach led to a 20,000EU fine.
    - Portuguese hospital: user access controls, data access management, and data collection controls necessary to ensure privacy leading to a 40,000EU fine.
  - CCPA
  - NY DFS
  - HIPAA
- **Contractual**
  - SLAs
  - Customers
- **Intersection Privacy and Security**
  - Securing data keeps it private
  - Ensure customer access and control
Audit Program: The Fourth Step

• Create audit plan based on compliance requirements
  — Objectives
  — Scope
• Internal audit:
  — Provides internal stakeholders assurance
  — Streamlines external audit
• External audit: provides customer assurance
Continuous Assurance: The Fifth Step

- **Continuous Monitoring:**
  - Threats evolve
  - Point-in-time audits no longer meet needs

- **Continuous Documentation**
  - Internal/External auditor assurance
  - Proves governance

- **Continuous Response**
  - Incident Response
  - Corrective Action Plan

- **Continuous Assurance**
Implementation: Organizing Assurance
Identify Internal Stakeholders

- **Risks are cross-departmental**
  - Compliance Officer
  - Senior Executive Team
  - Board of Directors
  - Requisitions
- **NERC Fined Duke Energy $10 million in January 2019.**
  - Lack of senior leadership oversight
  - No centralized Critical Infrastructure Protection (CIP) as required by the NERC Reliability Standards
  - Lack of benchmarks and key performance indicators
  - Lack of communication within the company
Assign Responsibilities and Accountabilities

- Who owns the application?
- Who owns the users?
- Who owns the monitoring?
- Who owns the response?
- Who owns the mitigation?
Assign Continuous Improvement Tasks and Metrics

- Who monitors alerts?
- Who responds to alerts?
- Who documents response?
- Who reviews the monitoring process?
Measuring Compliance Program Effectiveness
Mean Time Between Failures (MTBF)

- It has been ___ days since our last failure
- Shorter time means less effective controls
- Longer time means more effective controls
Difference in MTBF

- Do some systems have more failures on month-to-month comparison?
- Shows monitoring gap
- Control effectiveness issue
Mean Time to Repair (MTTR)

- How long does it take to respond to failure?
- Proves problem locating issues
- Lack of monitoring/governance
- Lack of resources
Percent Difference in MTTR

- Is there a month-to-month change in MTTR?
- Shows increased monitoring
- Shows greater resource management
Percentage of Scheduled Maintenance Activities Missed

- Divide number of devices not serviced by number of scheduled services
- Higher the percentage, better patching cadence
- Lower the percentage, worse patching cadence
Percentage of Network Devices Not Meeting Configuration Standards

• Divide number of incorrectly configured devices by total number of devices
• Higher the percentage, better governance
• Lower the percentage, more governance needed
Measuring Supply Chain Monitoring
Vendor Supplied Reports

- Self-assessment questionnaires
- External audits
- SOC 2 Reports
Reported Incidents

• 48% of 2018 healthcare breaches due to uncontrolled/unmanaged 3\textsuperscript{rd} party access

• British airways breach caused through 3\textsuperscript{rd} party web app by leveraging javascripts.

• BCBS RI breach caused by vendor responsible for sending member benefits.
Common Problems
Vendors Are Just Like You

- IoT
- BYOD
- AI
- Legacy Systems
- Supply Chain Management
- Records Retention/Disposal
Teamwork Makes the Dream Work

- Communication between stakeholders
- Data ecosystem, not environment
- Continuous insights lead to continuous improvements
Automating the Process
More Data, Less Problems

• Manual processes lead to increase human error
• Added systems, networks, software, devices, and vendors make sampling overwhelming
• Automation allows for more data for better outcomes
Continuous Monitoring

• No more “point in time”
• Fewer security gaps
• Better compliance outcomes
Continuous Documentation

• Putting the G in GRC
• Focus on proving response and mitigation
• Document VRM
Continuous Assurance

• Provide confidence to upstream supply chain
• Streamline audit documentation gathering
• Open communication between all stakeholders
Final Thoughts
How to implement?

• Assign responsibilities
  • Accountability
  • Key Stakeholders
  • Continuous assurance strategy

• Continuous assurance and oversight key tasks
  • Analyze
  • Report
  • Respond
  • Continuously update

Key Stakeholders
- Information Security Leaders (CISOs, etc.)
- Privacy Leaders (CPOs, etc.)
- Compliance Leaders (COOs, etc.)
- Risk Management Leaders (CMOs, etc.)
- Board and Executive management
- Business Unit management
- Supply Chain management
- IT management
- Physical Security/Safety management
- Internal audit
Automation Is Best Security and Compliance

Best Practice

• Increased risk and severity of data breaches
• “Trust but Verify”
• Communication is key
• Automation strengthens security
• Continuous monitoring for continuous documentation
• Continuous assurance rather than point-in-time process
Thank You