Top Security and Risk Management Trends for 2019 and Beyond

Steve Riley
Sr. Director, Analyst—Cloud Security
3.5x

Increase in organizations with 50% of their data in the cloud 2018-2020
93% are dealing with rogue cloud app usage
85%

Are interested in replacing passwords with new forms of authentication
More than 80% of enterprise web traffic will be encrypted through 2019
The Controls of Security Are Rapidly Shifting and Your Focus Needs to Shift to New Approaches
External Mega Trends Beyond Your Control

- Skills Gap
- Attackers
- Regulation and Privacy
- Cloud Application Scale and Complexity
Internal Mega Trends that Support Success

- Perfect prevention and authentication is not possible — Plan, Detect, Respond
- Cloud delivery is one way to address the skills and scale gap
- Need to step up our game in communication
2019 Trends
Trend 1
1.5 million
Unfilled global cybersecurity roles expected by 2020

Trend 1: Fusion of Products and Services
Trend 2
33% increasing investment in cloud

35% decreasing investments in datacenter

Source: Oracle and KPMG Cloud Threat Report 2019
Trend 2: Cloud Center of Excellence Emerges
Four Primary Areas of Investment

- Cloud Security Posture Management (CSPM)
- Cloud Workload Protection Platforms (CWPPs)
- Cloud Access Security Brokers (CASB)
- Chief Cloud Architect & SecDevOps

Infrastructure
Platform
Software
People & Process
Trend 3
49%
Expect to store the majority of their data in a public cloud by 2020

Source: Oracle and KPMG Cloud Threat Report 2019
71% Report that the majority of their cloud-resident data is sensitive

Source: Oracle and KPMG Cloud Threat Report 2019
Trend 3: Data Security Governance Framework
DSG Framework

Don’t Start Here!

4 Implement Security Products

5 Orchestrate Policies for All Products

Crypto  DCAP  DLP  CASB  IAM  UEBA

DBMS  Big Data  Files  Cloud  Endpoint
DSG Framework

1. Balance Business Needs Versus Risks
2. Identify, Prioritize and Manage Dataset Life Cycles
3. Define Data Security Policies
4. Implement Security Products
5. Orchestrate Policies for All Products

Start Here!

Business Stakeholders

- Business Strategy
- Governance
- Compliance
- IT Strategy
- Risk Tolerance

Prioritize Datasets

- Data
- People
- Analytics

- Crypto
- DCAP
- DLP
- CASB
- IAM
- UEBA

- DBMS
- Big Data
- Files
- Cloud
- Endpoint
Trend 4
83.9% of phishing attacks targeted credentials for financial, email, cloud, payment, and SaaS services.

Trend 4:
Dawn of Passwordless Authentication
35% of smartphones will adopt more than one biometric authentication method by 2022.

Passwordless Authentication

Windows Hello

Security Key by Yubico
Trend 5
70% of organizations are unable to process more than 60% of their security event data.

Source: Oracle and KPMG Cloud Threat Report 2019
Trend 5: Security Operations Center Revitalization
50% of all SOCs will transform into modern SOCs with integrated incident response, threat intelligence and threat hunting capabilities by 2022.
Biggest Challenges

**New**

- Staffing
- Adopting new tools
- SIEM vs. EDR
- Or Outsource

**Renewed**

- Integrating threat intel
- Consolidating alerts
- Establishing playbooks
- Automating workflow
- SOAR
Trend 6
Trend 6: Carta Proliferates
Examples

- Intrusions detection inside the LAN
- Internal protection for email
Trend 7
90% of large enterprises CISOs expected to present security issues to business leaders.
Trend 7:
Risk Appetite Statements Emerge
The Simple Story

We do these things

To support these principles

So we can help manage these risks

So you can help accomplish your goals
Sample Risk Appetite Statement

National Rail System has no appetite for safety risk exposure that could result in injury or loss of life to public, passengers and workforce. All safety targets are met and improved year on year. In the pursuit of its growth and modernization objectives, the NRS is willing to accept risks that may result in some financial loss.
Think Differently

Explore New Options

Challenge Assumptions
Top Security and Risk Management Trends for 2019 and Beyond

Steve Riley
Sr. Director, Analyst—Cloud Security