SAFEGUARDING IN A DIGITAL WORLD

CYBERSECURITY STRATEGIES FOR PRIVATE EQUITY AND PORTFOLIO COMPANIES

JUNE 6, 2024

RSM

Your presenters

Ty Smith

Director, RSM

Ty leads the private equity practice for RSM’s security group and specializes in vCISO engagements.

With 10 years of experience serving private equity and other industries, Ty and his team bring cyber risk mitigation strategies at the fund and portfolio level to maximize investment in the private equity life cycle.

George Kohlhofer

Principal, RSM

George leads RSM's cyber recovery and remediation practice globally.

With over 25 years of consulting and technology experience, George and his team deliver a wide range of technology solutions to solve complex business and technology challenges.

David Llorens

Principal, RSM

David leads RSM's cyber response, testing and engineering practice globally.

With over 20 years of consulting and technology experience, David and his team deliver a wide range of cybersecurity solutions to solve complex business challenges, improve resilience, and reduce risks or compromise.

Agenda

- Private equity outlook
- Cybersecurity trends and current state
- Case study
- Recommendations
- How RSM can help

Private equity outlook

RSM

2024 private equity outlook

PE deal activity outlook

01

- 2023 decline: Deal volume fell by 24% in 2023 due to rising interest rates and slowing growth, but Q4 showed improvement.
- Worst-hit sectors in 2023: Technology, media and telecom (TMT), retail and energy.

02

- Expected rebound: These sectors are projected to recover in 2024.
- Long-term trend: Expected to resume in 2024 barring major geopolitical or macroeconomic disruptions.

03

- License and vendor rationalization: Efforts to reduce overlap and achieve volume discounts.
- Outsourcing: Growth in onshore and offshore outsourcing, particularly in managed IT.
- Automation: Focus on labor rationalization and cost reduction within growth strategies.

04

- ***TREND*** - Global expansion: Increasing cross-border deal making and expansion of office footprints.
- ***TREND*** - Back-office technology: Adoption of cloud-based platforms and outsourcing to improve efficiency and reduce costs.

05

- ***TREND*** - ESG: Ongoing reevaluation of environmental, social and governance strategies.
- ***TREND*** - Cybersecurity: Balancing threat intelligence and insurance to protect against cyber threats.

Source: RSM's 2024 Private Equity Outlook report

Cyber risk by the numbers

Preparing for the evolving trends of cybersecurity

Identity is the new perimeter

Changing borders of the workplace and IT landscape have forced a shift from network boundaries to a focus on digital identity defenses.

Tomorrow's cyber workforce is being built today

The war for talent is driving investments into internal staff development through retooling and upskilling the workforce.

Responsibility must align with "as a service"

Complex vendor ecosystem requires constant alignment and communication while adapting to evolving technologies and regulatory needs.

Automation will drive action over alerts

Automation will need to extend beyond detection and orchestration to drive decisioning in near real time.

Data will fuel risk and opportunity in cyber

Data will serve as an increasingly valuable business and cyber asset but with tightening regulation and growing risk to organizations.

Cyber service and platform markets will consolidate

Anticipate vendor convergence to expand core capabilities, drive margin, enhance operations and unify disparate solutions.

Recent cyberattacks from the headlines

March 2022	August 2022	May 2023	September 2023
OpenAI	**Atlassian**	**Progress Software (MoveIt)**	**MGM**
Advanced persistent threat	*Technology stack and supply chain*	*Technology stack and supply chain*	*Ransomware*
Bug in ChatGPT's open-source library resulted in leak of personal data of customers	Data breach related to staff and company facilities and potential exposure of its customers' data	Data breach and service takeover exposed company and personal data of tens of millions of individuals	Names, driver's licenses, and financial account information stolen and held for ransom; hotels operations also locked down

2023 cyberattacks by the numbers

Frequency of malware

More than [1]

450,000

new malware programs are detected daily

Frequency of phishing emails

3.4 billion

phishing emails are sent everyday totaling 1.2% of all email traffic[2]

Average downtime from ransomware

20+ days

of average system downtime and business interruption from a ransomware attack[3]

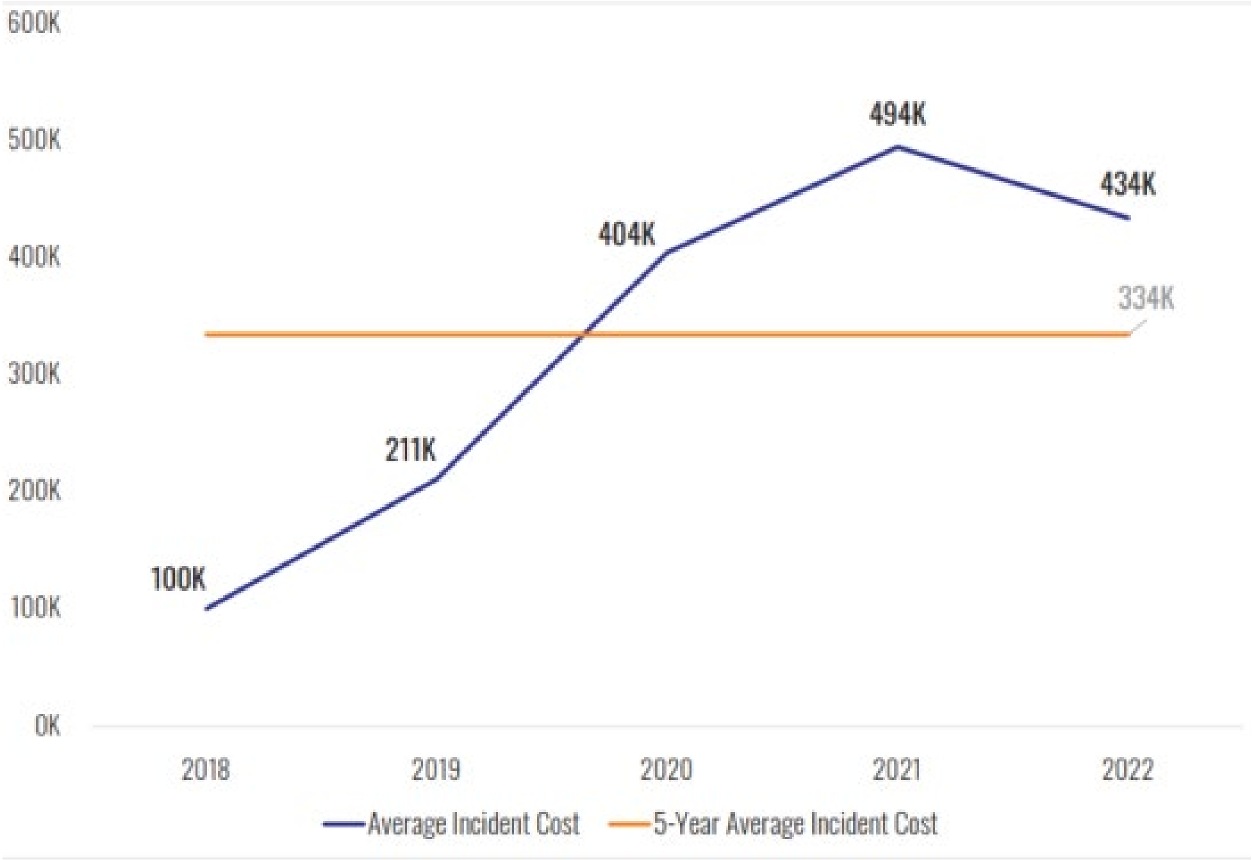
Average cost of a breach

Global average cost in 2023

$4.45MM

an increase of 15% over the last 3 years[4]

Average incident costs



Average Incident Cost – All Ransomware Claims
SMEs
(N=2,556)

Figure 32

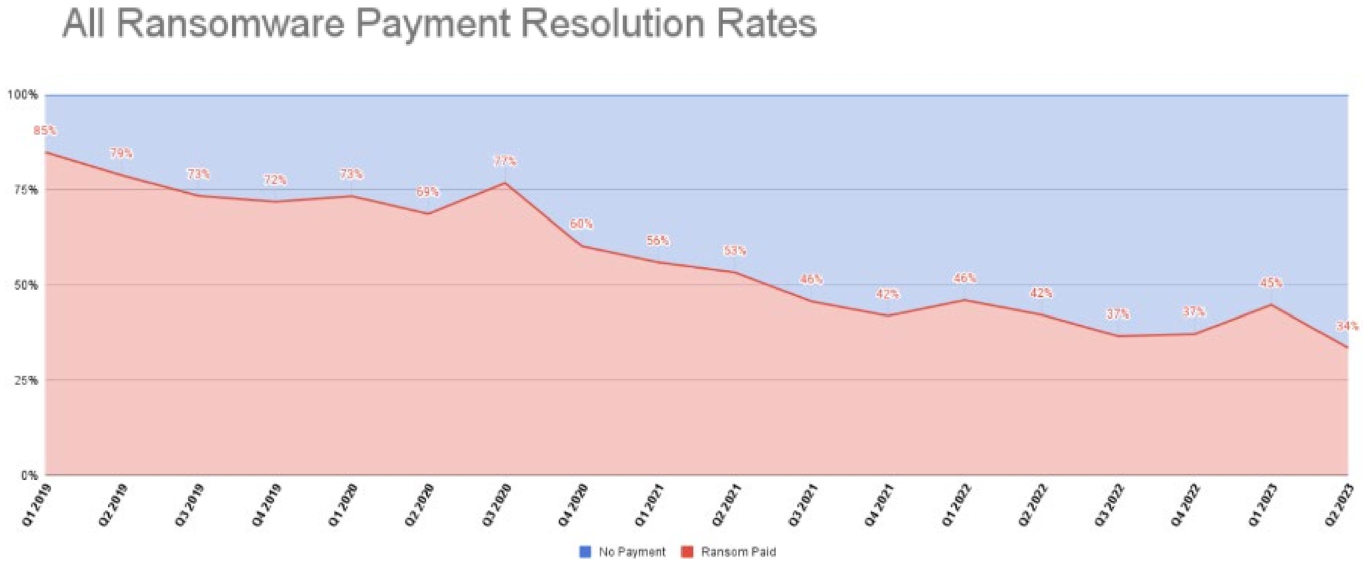
Incident costs may include:

- Business interruption
- Legal fees
- Forensic fees
- Recovery fees
- Regulatory reporting
- Negotiations

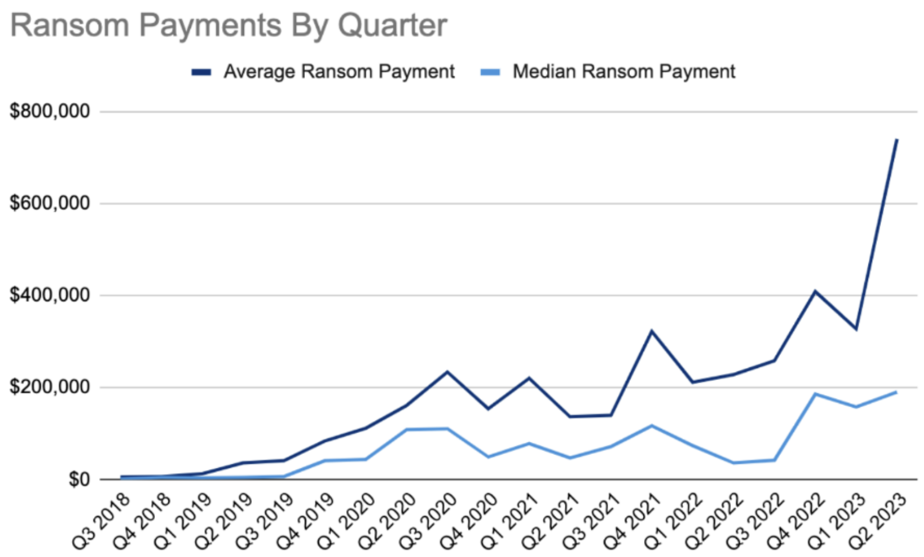
Source: 2023 Net Diligence Cyber Claims Study

Ransom payment rates falling

Payment rates are dropping; Ransom amounts are increasing



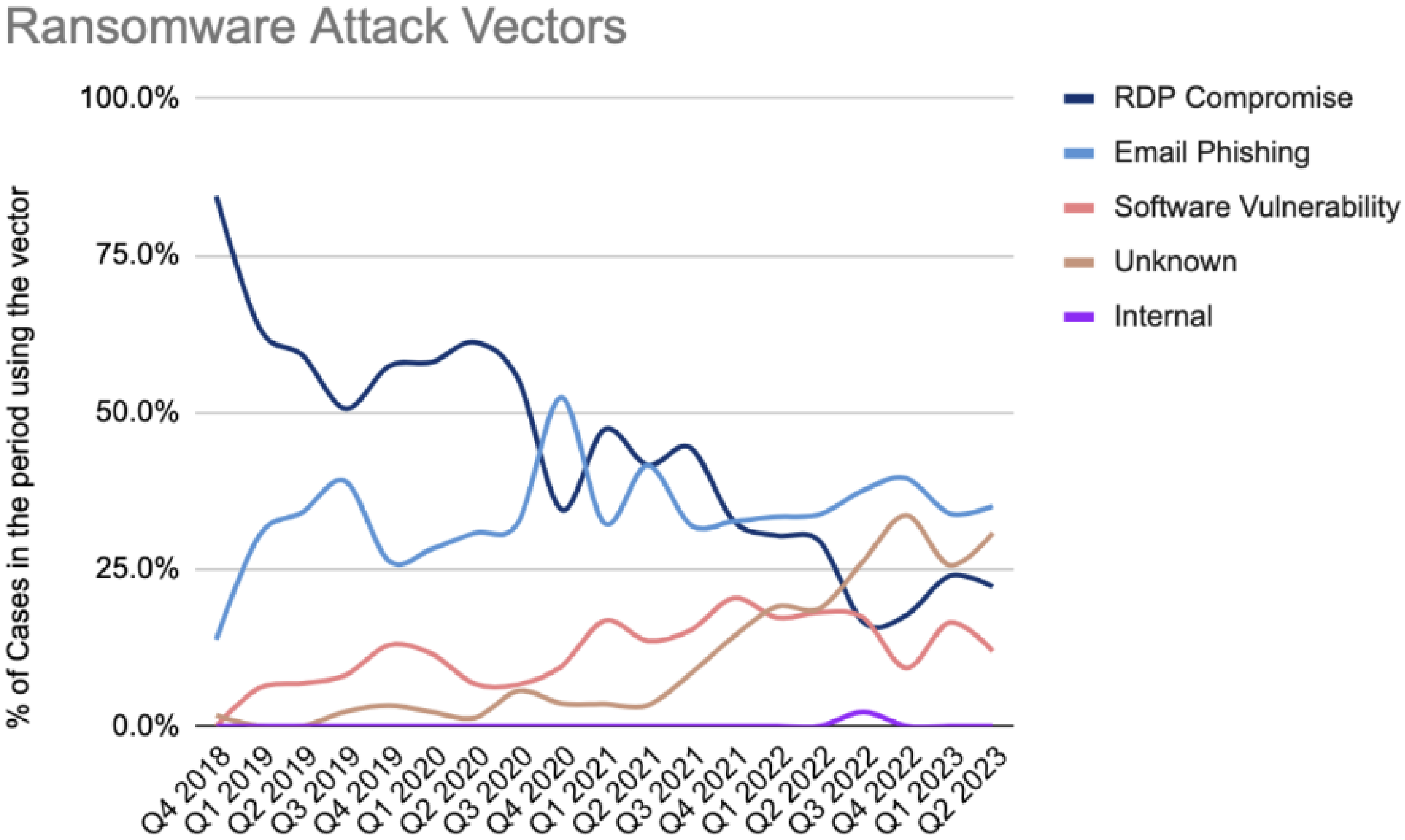
All Ransomware Payment Resolution Rates



Ransom Payments By Quarter

Source: Coveware -Ransom Monetization Rates Fall to Record Low

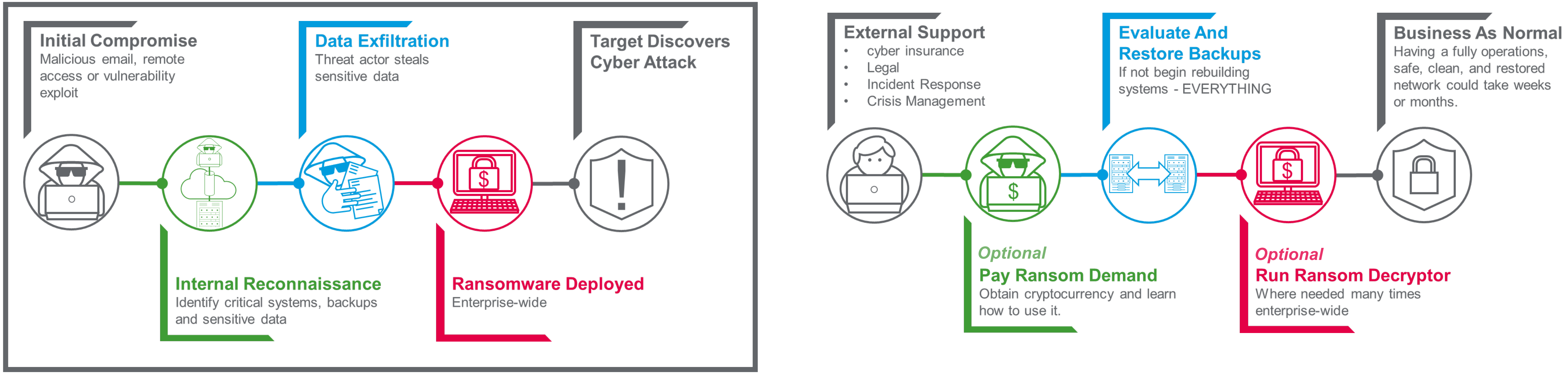
Poor practices regularly exploited



Case study

Ransomware and recovery timeline

The average length of interruption after ransomware attacks on organizations in the United States in 2023 was 22 days*



Initial Compromise
Malicious email, remote access or vulnerability exploit

Internal Reconnaissance
Identify critical systems, backups and sensitive data

Data Exfiltration
Threat actor steals sensitive data

Ransomware Deployed
Enterprise-wide

Target Discovers Cyber Attack

External Support

- cyber insurance
- Legal
- Incident Response
- Crisis Management

Optional
Pay Ransom Demand
Obtain cryptocurrency and learn how to use it.

Evaluate And Restore Backups
If not begin rebuilding systems - EVERYTHING

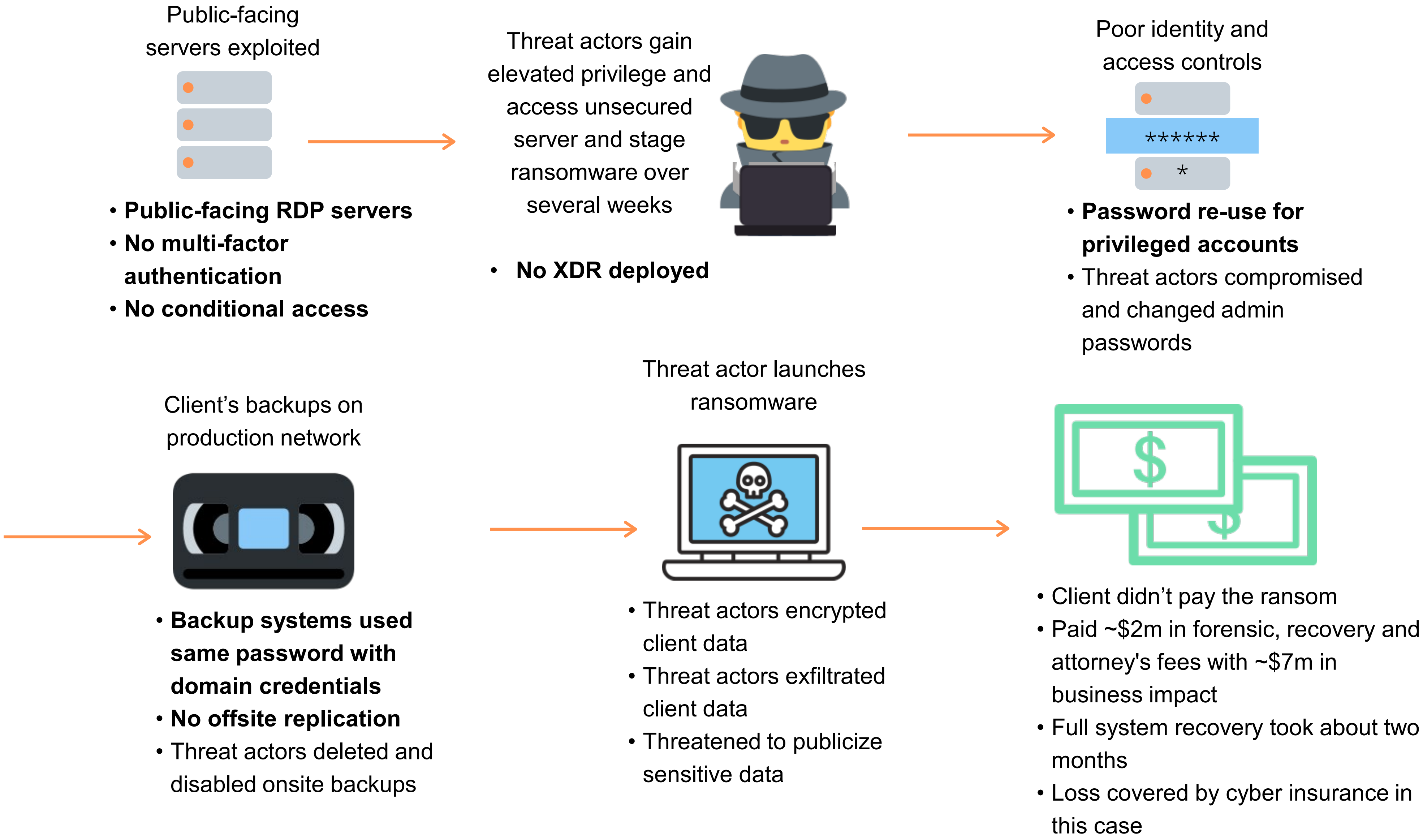
Optional
Run Ransom Decryptor
Where needed many times enterprise-wide

Business As Normal
Having a fully operations, safe, clean, and restored network could take weeks or months.

This timeline could take days, weeks or even months and have severe business impacts.

Source: Cignet

Standard recommendations



Public-facing servers exploited

- **Public-facing RDP servers**
- **No multi-factor authentication**
- **No conditional access**

Threat actors gain elevated privilege and access unsecured server and stage ransomware over several weeks

- **No XDR deployed**

Poor identity and access controls

- **Password re-use for privileged accounts**
- Threat actors compromised and changed admin passwords

Client's backups on production network

- **Backup systems used same password with domain credentials**
- **No offsite replication**
- Threat actors deleted and disabled onsite backups

Threat actor launches ransomware

- Threat actors encrypted client data
- Threat actors exfiltrated client data
- Threatened to publicize sensitive data

- Client didn't pay the ransom
- Paid ~$2m in forensic, recovery and attorney's fees with ~$7m in business impact
- Full system recovery took about two months
- Loss covered by cyber insurance in this case

Recommendations

Standard recommendations

Activity	Risk	Description
Technical cyber assessments	HIGH	Penetration test, insider threat analysis, threat hunting, cloud security assessment, etc.
Managed security	HIGH	24/7 managed EDR/XDR for around the clock monitoring and remediation as needed.
Perimeter security	HIGH	Implement multi-factor authentication for all internet facing technology and remote access. Upgrade aging hardware and/or review/apply rules and configurations focused on security.
Immutable backup	HIGH	Implement backup solution following best practices with immutability and full system restorability. Periodically test of backups and recovery timelines.
Privileged access management	HIGH	Create a tiered privileged access strategy for added security and buffer between device layers.
Identity and access management (IAM) hardening	MEDIUM	Review and harden active directory, cloud entitlements and remote access to different environment/policies for added security.
Email security hardening	MEDIUM	Conduct a thorough security assessment and hardening of your email environment based on industry standards.
Fund level cyber governance	MEDIUM	Implement cyber standards across the portfolio and utilize dashboards to visualize and track portfolio risk reduction.

RSM cyber services

Across a spectrum of services

Assess ◆ Advise ◆ Implement ◆ Manage

SERVICES

Attack surface management

Identify and reduce attack surface through continuous proactive management

- Vulnerability management
- Penetration testing and red teaming
- Asset discovery and management
- Technical cyber compliance programs

Resilience and recovery

Understand cyber resilience obligations and prioritize recovery operations

- Impact analysis
- Business continuity and disaster recovery
- Application and system rationalizations
- Third party risk management

Secure cloud

Embark on your cloud journey in a controlled and secure manner

- Cloud posture management
- Platform design, development and deployment
- Secure operations and administration
- Cloud infrastructure entitlements management

Architecture and engineering

Manage the risks of today's boundary-less environment

- IoT and operational technologies
- Industrial control systems
- Zero-trust and enterprise architecture
- Standards and runbooks
- Cyber solution engineering
- Security tools and technologies

Application security

Drive secure practices throughout the application development life cycle

- SecDevOps
- Secure code analysis
- Web app security testing
- Secure design principles
- Data classification and protection
- Continuous penetration test

Detect and respond

Effectively and efficiently identify and quickly respond to incidents

- *RSM Defense*^{TM} – managed security
- Security operations
- Threat intelligence
- Digital forensics and incident response
- Endpoint detection and response

Strategy and risk

Design and implement transformative cyber programs

- Maturity and risk assessments
- Policies and procedures
- Program design and management
- Framework design
- Virtual CISO
- Security awareness training
- Cyber workforce development

Compliance and governance

Decipher framework, regulations and standards compliance

- Assurance, accreditation, and certification (i.e., PCI, FedRamp, CMMC, HiTrust, etc.)
- Third-party risk
- Governance, risk and compliance (GRC)
- Privacy

Digital identity

Securely manage human and device identities across your universe

- Governance and administration
- Privilege access
- Authentication and authorization
- Identity threat detection and response
- User behavior analytics

Emerging technologies

Making sense of security implications from technology innovations to prioritize resources

- Artificial Intelligence
- Autonomous vehicles
- Metaverse and augmented reality
- Virtual power plants (VPP)

Elevating managed security

RSM DEFENSE

ALWAYS ON

24x7 security analysts monitoring our clients' environments for suspicious and confirmed threats

FOREVER VIGILANT

Leveraging automation workflows, reducing MTTD and dwell time for our clients to speed in faster response and recovery

INFORMED RESPONSE

Threat intelligence is integrated into everything we do, aids in prioritizing risks and determining the correct course of action

CAPABILITIES

Security event monitoring

Near real-time security monitoring of client environments, correlating events and analyzing potential threats leveraging our cloud-based monitoring platform.

Attack surface reduction

Our fully managed vulnerability capabilities including continuous scanning execution across the stack, file and configuration monitoring, false positive analysis, and detailed remediation actions.

Threat intelligence

Fully integrated open and closed intelligence sources helps influence the decision-making process for our analysts.

Network traffic analyses

Collecting netflow to provide additional intelligence in threat investigations.

Automated response

Leveraging automated playbooks, we can perform predefined scripted remediation activities.

Endpoint security

Identifying risks and behavioral anomalies affecting your technology endpoints, continually tuning the system, and working directly with our incident responders.

IoT/device monitoring

Providing threat monitoring of clients ICS environments utilizing a lightweight collector meant for plant and health care environments.

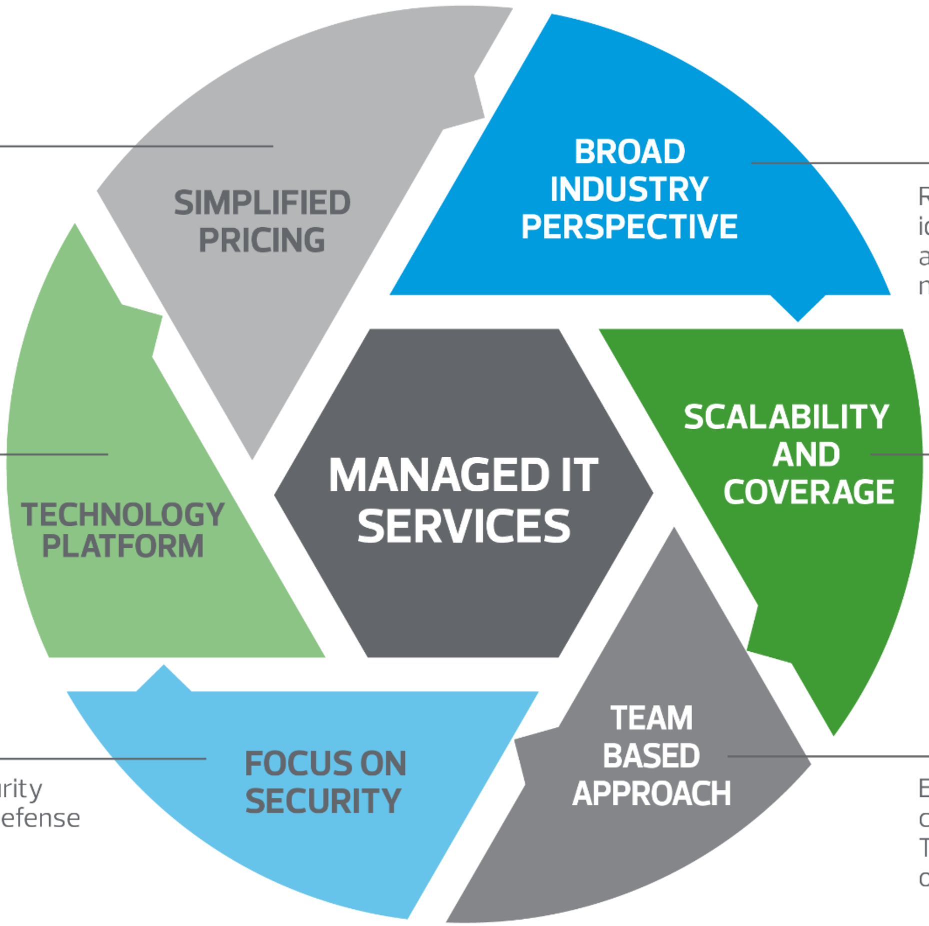
Brand safeguarding

Monitoring cybersquatting activity and protecting your domain name from typosquatting, helping to safeguard your reputation.

Managed services value proposition

RSM

Assess ◆ Advise ◆ Implement ◆ **Manage**



Our programs offer a predictable monthly spend that scale easily to accommodate the evolving IT needs of startups to established commercial and non-profit organizations.

Our MITS technology platform integrates best-of-breed 3rd party solutions across service management, IT operations and monitoring, backup & recovery, end user learning, and cyber security.

Our program enhances your security posture by integrating our RSM Defense service to identify and neutralize real-time threats.

RSM's advise, deliver, manage approach identifies the ideal IT solutions to accommodate your specific industry needs and regulations.

Our clients have access to 1000+ technology consultants across a variety of disciplines at 90 locations in the US, Canada, and International.

Every client is serviced by a team consisting of a an RSM owner, Client Technology Advisor, local staff, and our national centers of excellence.

Question and answers

RSM

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute assurance, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent assurance, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.