KirkpatrickPrice

The Rise of Ransomware: Best Practices for Prevention and Mitigation

KirkpatrickPrice

Welcome

Joseph Kirkpatrick is the Managing Partner at KirkpatrickPrice and holds the CPA, CISSP, CISA, CGEIT, CRISC, and QSA certifications, specializing in data security, IT governance, and regulatory compliance. He enjoys helping our clients and stakeholders by navigating them through the complex maze of compliance and regulatory requirements.

KirkpatrickPrice

KirkpatrickPrice is a licensed CPA firm and PCI QSA, providing assurance services to clients worldwide. The firm has over 14 years of experience in information assurance by performing assessments, audits, and tests that strengthen information security and compliance controls.

Regulatory Compliance

- Consulting
  - Policy and Procedure
  - Risk Assessment
  - Internal Audit Plan Development
- Readiness Audits

Information Security

- Guidance and Audit Services
  - SOC 1, SOC 2, SOC 3
  - PCI DSS
  - HIPAA
  - HITRUST
  - GDPR
  - ISO 27001/27002
  - FISMA

CyberEdge Group Survey

- Surveyed 1,200 IT security practitioners and decision makers across 17 countries
- 55% suffered a ransomware infection in 2017
- 61.3% did not pay the ransom
  - 8% lost their files
  - 53.3% recovered their files through backups
- 38.7% paid the ransom
  - 19.1% recovered their data
  - 19.6% lost their data

City of Atlanta—March 22, 2018

There has been a notable focus so far in 2018 on ransomware targeting government services, schools, and hospitals.

- This attacker, SamSam, is known for choosing targets most likely to pay the ransom, in this case $51,000
- The SamSam group has extorted more than $1 million from 30 organizations in 2018

David Jordan, CISO, Arlington County

"…start considering cybersecurity on the same level as public safety. A smart local government will have fire, police, and cybersecurity at the same level."

New York Times

Practice Disaster Recovery and Business Continuity

- Are you able to recover from a disaster?
  - Do non-IT resources have procedures to follow in the case of widespread outages?
  - Are your backups tested? Is there an offline copy?

- Can you continue operation during an outage?
  - Are manual procedures available and practiced?
  - Have you conducted a business impact analysis in order to find the critical processes that would need to continue on a daily, weekly, monthly basis?

The Business Continuity Hall of Fame

- Linda Cunningham
- Administrative Assistant to the VP of Patient Care Services
- Princeton Community Hospital
- Maintained an archive of paper templates that she printed and saved in a binder

Why is ransomware successful?

Phishing is the primary method of attack

- 53% of all email threats are phishing
- 75% of them contain a malicious URL

Is your workforce your weakest link or your first line of defense?

Microsoft Security Intelligence Report

Why is ransomware successful?

Millennials are becoming a bigger portion of our workforce

- 18% of adults over 70 are victims of fraud
- 40% of adults aged 20-29 are victims of fraud

Are you providing the necessary training to the newest members of our workforce?

Federal Trade Commission

Why is ransomware successful?

A growing apathy in our culture

- Accenture surveyed 912 qualified employees of health providers and payer organizations in the U.S. and Canada
- 18% responded they would be willing to sell confidential data to unauthorized parties for as little as $500 to $1000
- 24% of the health employees said they actually know of someone in their organization who has sold their credentials or access to an unauthorized outsider

Are you building an internal control environment that will embrace, monitor, and enforce ethical practices?

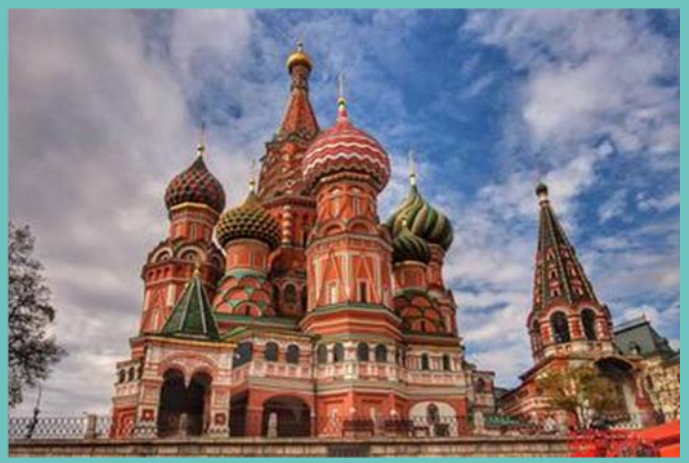
Why is ransomware successful?

Security configurations are not tested and validated

- The Zenis ransomware strain targeted weaknesses in Remote Desktop Protocol
- Back to the City of Atlanta, they previously did not patch for the NSA toolkit vulnerability in a timely fashion

Do those charged with governance ensure that IT and Security are maintaining configurations according to best practices?

Why is ransomware successful?



Nation-states are behind the attacks and have a goal of disrupting public services

- Russian cyber operatives
- Russian Federal Security Service
- North Korea
- China

Connect With Us

- Subscribe to our blog for regular industry updates, tips, and best practices
- Visit our library of recorded webinars
- Check out our free video resources and subscribe to our YouTube Channel
- Connect with us on LinkedIn, Twitter, and Facebook

Questions?

Joseph Kirkpatrick
joseph@kirkpatrickprice.com
800.977.3154 x101