THE POWER OF BEING UNDERSTOOD

AUDIT I TAX I CONSULTING

Agenda

- Security essentials
- Year in review
- College/university challenges
- Recommendations

RSM

About me

Matt Franko

Director, Risk Advisory Services
matthew.franko@rsmus.com
(216) 927-8224

- 11+ years in cybersecurity
- Provides security, privacy and risk related services to several Ohio universities and colleges.
- PCI QSA, CISSP

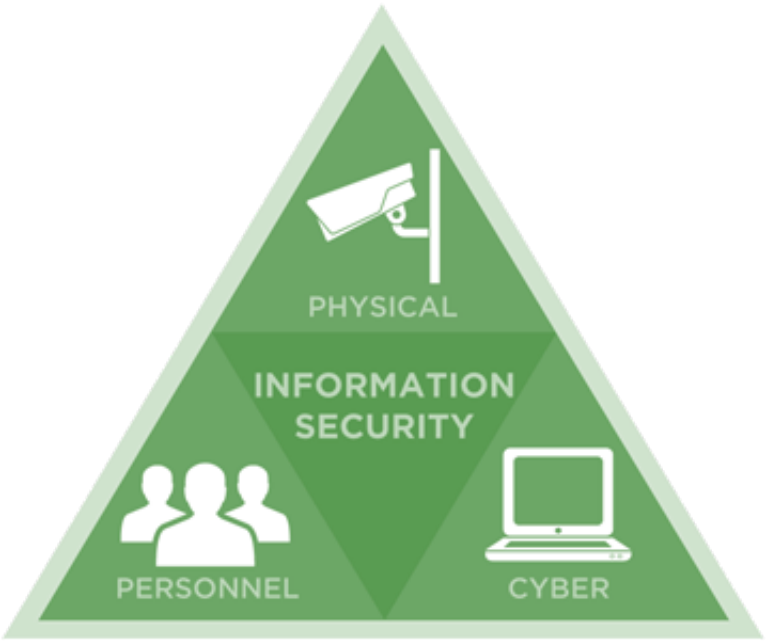
CISSP® Certified Information Systems Security Professional

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

RSM

Security essentials

- To protect assets, you need strong controls in three primary areas:
  - Personnel/process
  - Cyber
  - Physical
- Failure in any of the three primary controls can cause a breach of your assets.
- Failure of the two wrappers can either increase the impact of the breach or further cause problems with the primary controls



RSM

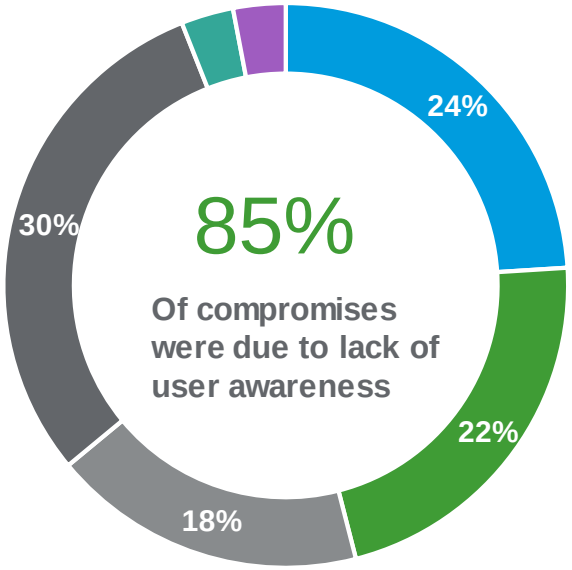
Year in review: top attack vectors

Top external attack vectors

- Phishing
- Weak passwords

Internal pivot points

- Weak passwords
- Outdated systems
- Default passwords
- Sensitive data insecurely stored



*$166/Record

*Per IBM's 2018 Cost of a Data Breach Study

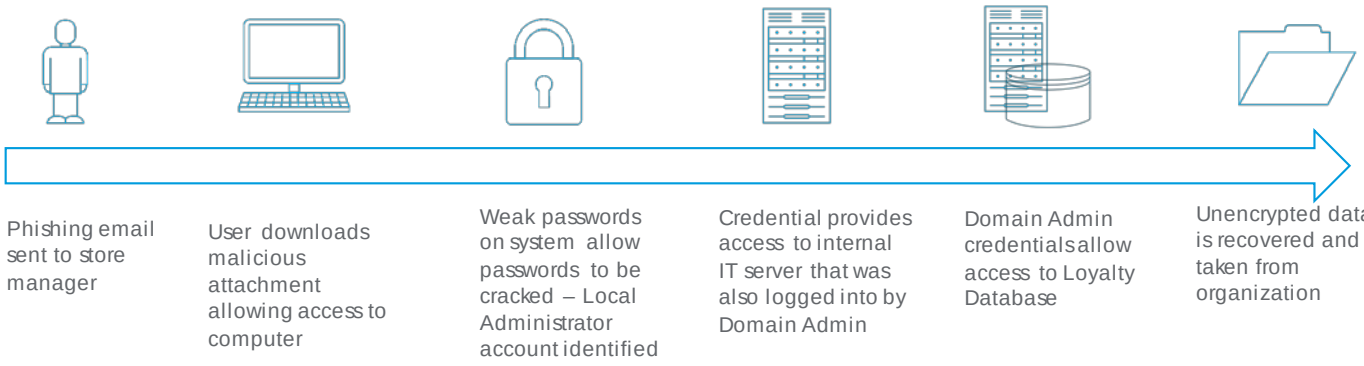
How are hackers getting to information?

Get the initial foothold

- Phishing
- Weak passwords
- Default/missing credentials

Pivot to the data

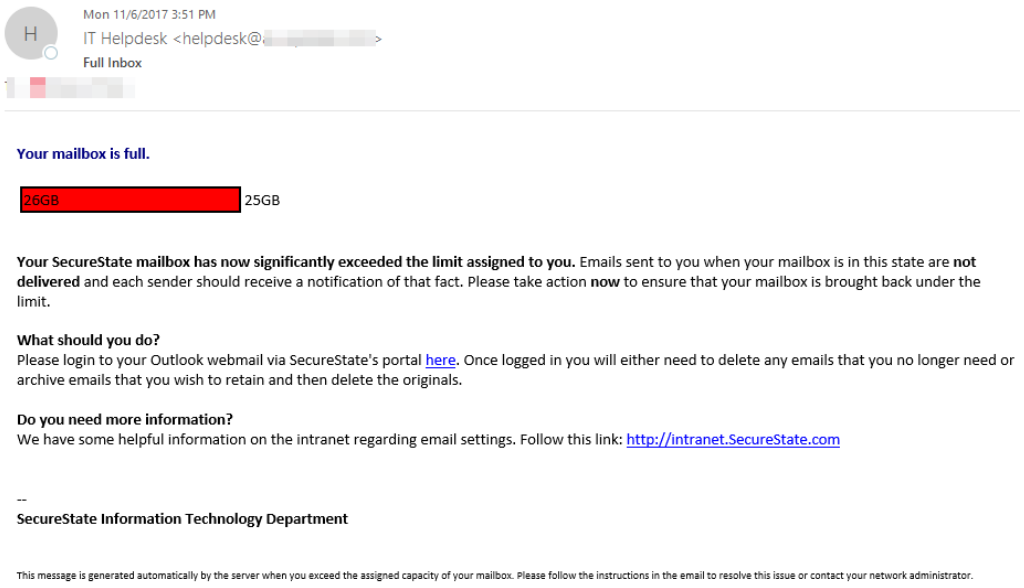
- Clear text passwords in memory
- Improper network segmentation
- Sensitive data left unprotected at rest



RSM

Office 365 type attacks

- Record retention



Mon 11/6/2017 3:51 PM
IT Helpdesk <helpdesk@[redacted]>
Full Inbox

Your mailbox is full.

26GB 25GB

Your SecureState mailbox has now significantly exceeded the limit assigned to you. Emails sent to you when your mailbox is in this state are **not delivered** and each sender should receive a notification of that fact. Please take action **now** to ensure that your mailbox is brought back under the limit.

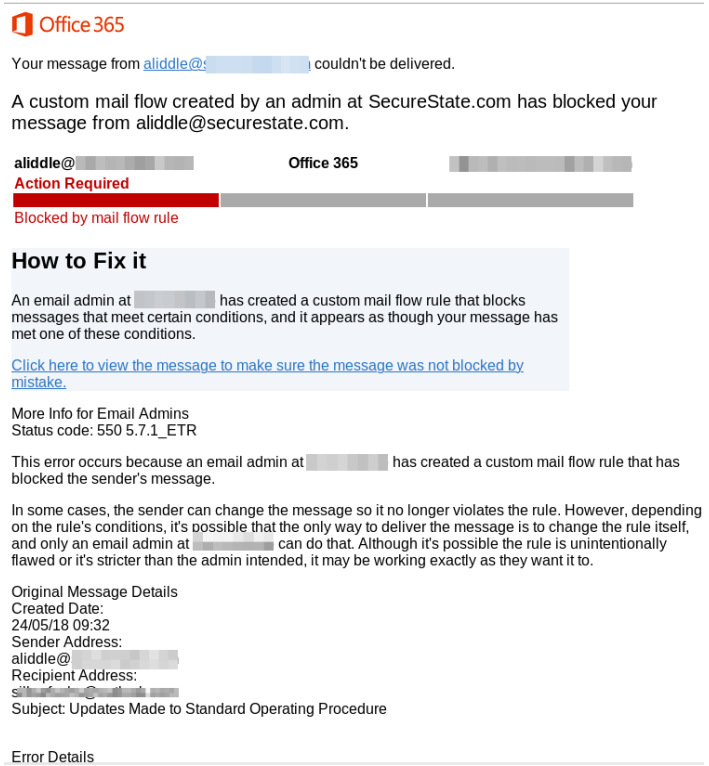
What should you do?
Please login to your Outlook webmail via SecureState's portal here. Once logged in you will either need to delete any emails that you no longer need or archive emails that you wish to retain and then delete the originals.

Do you need more information?
We have some helpful information on the intranet regarding email settings. Follow this link: http://intranet.SecureState.com

--
SecureState Information Technology Department

This message is generated automatically by the server when you exceed the assigned capacity of your mailbox. Please follow the instructions in the email to resolve this issue or contact your network administrator.

- Outlook rules



Office 365

Your message from aliddle@[redacted] couldn't be delivered.

A custom mail flow created by an admin at SecureState.com has blocked your message from aliddle@securestate.com.

aliddle@[redacted] **Office 365** [redacted]
Action Required
Blocked by mail flow rule

How to Fix it

An email admin at [redacted] has created a custom mail flow rule that blocks messages that meet certain conditions, and it appears as though your message has met one of these conditions.

Click here to view the message to make sure the message was not blocked by mistake.

More Info for Email Admins
Status code: 550 5.7.1_ETR

This error occurs because an email admin at [redacted] has created a custom mail flow rule that has blocked the sender's message.

In some cases, the sender can change the message so it no longer violates the rule. However, depending on the rule's conditions, it's possible that the only way to deliver the message is to change the rule itself, and only an email admin at [redacted] can do that. Although it's possible the rule is unintentionally flawed or it's stricter than the admin intended, it may be working exactly as they want it to.

Original Message Details
Created Date:
24/05/18 09:32
Sender Address:
aliddle@[redacted]
Recipient Address:
[redacted]
Subject: Updates Made to Standard Operating Procedure

Error Details

Specific challenges for colleges and universities

- ✓Disparate departments doing their own thing or don't know their responsibilities
- ✓Rogue systems and servers being deployed
- ✓Sensitive data on insecure laptops/mobile devices
- ✓Soft physical security targets
- ✓Complications translating/implementing critical incident and business continuity requirements

RSM

University threats

Critical data

- Personally identifiable information
- Bank account information
- Cardholder data
- Protected health information
- Research data
- Donor information

Open environments

- Freedom of information

Increased exposure

- Students with access and skill set

The road from computer whiz to creepy hacker: North Royalton man accused of spying on thousands

RSM

Key areas to limit risk

- **Incident response planning**
  - Identify vulnerabilities/risks within the environment and develop a plan for remediation
- **User education and awareness**
  - Primary source of compromise in environments
  - Vigilance, password complexity
- **Segmentation**
  - Secure research environments
  - Sensitive data storage areas with increased access controls
  - Security controls based on risk presented by each department
- **Establishing a physical business impact analysis and risk assessment program**
  - Determine and regularly review potential impacts to a university arising from disruptive events

RSM

Board level discussion points

- What are we doing to protect our data?
- Do we know where our sensitive data is stored, processed, transmitted and accessed?
- What data elements are we collecting?
- Has internal audit been engaged to conduct an IT controls review?
- How are we managing regulatory/compliance requirements?

RSM

Board level discussion points

- **Monitor metrics**
  - Look for systemic issues. Are we getting better or worse? What is the root cause?
- **Show me our phishing assessments from the last four quarters**
  - Quarterly reinforcement
- **How are we educating users on using better passwords and are we testing this?**
  - Are we running password audits to determine where areas of weaknesses exist?
  - Have we or when will we move to 12 character passwords?
  - How mature is our cyber awareness program? Does it match our policies?

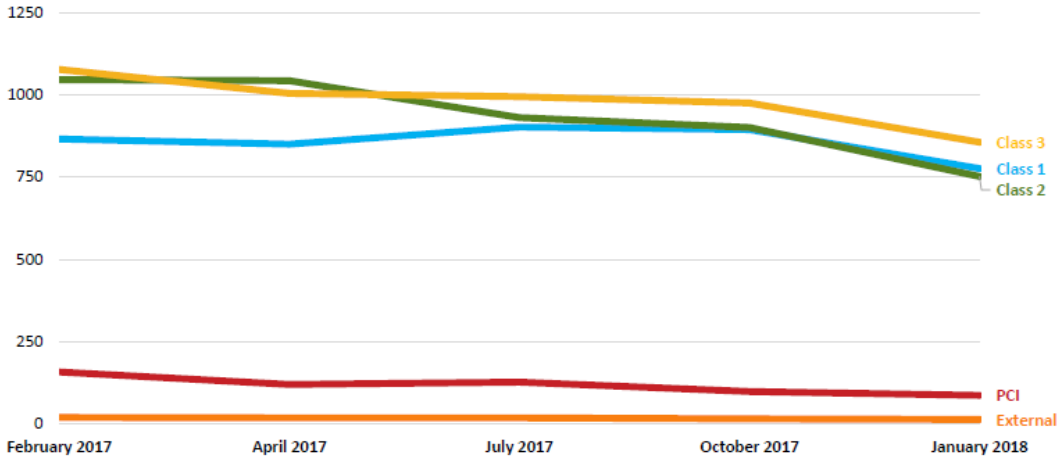


Figure 1: Vulnerability Trending by Asset Class

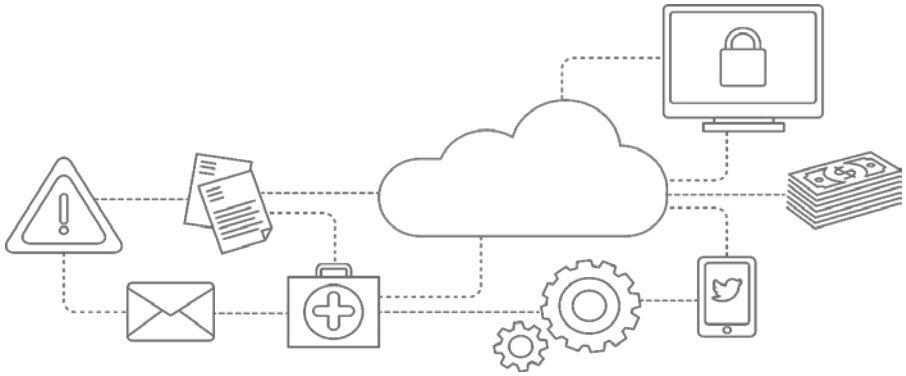
Key takeaways

- Security is not just IT/cyber related
  - To properly secure an asset (people, technology, physical data) you must include three facets – physical, cyber and personnel
- Targeting weaknesses in personnel remain the easiest way to gain unauthorized access
- Incident response planning and testing is key in limiting damages
- Remember your discussion points – ask questions and be curious

RSM

Questions

Consulting services



In addition to tax and audit, RSM offers cost-effective risk, financial, and technology and management advisory services.

Financial advisory

- Transaction advisory
- Valuation
- Litigation and dispute advisory
- Forensic accounting and fraud investigations
- IPO readiness
- Real estate advisory

Risk advisory

- Internal audit/Sarbanes-Oxley advisory
- IT audit
- Security and privacy
- Governance, risk and compliance and enterprise risk management
- Contract compliance
- Service organization control assurance
- Regulatory compliance
- ERP risk advisory

Technology and management consulting

- Management consulting
- ERP and CRM
- Cloud computing
- Business intelligence
- Content management and collaboration
- Application development and integration
- Infrastructure
- Managed services
- Business process outsourcing

RSM

RSM US LLP

+1 800 274 3978
www.rsmus.com

www.rsmus.com

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, 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.

For more information, visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.