Securing Communication & Collaboration in the Cloud

Common Concerns & Best Practices

Cassandra Young
O365/Azure Systems Administrator @ ISC

“If everything seems under control, you’re just not going fast enough.”

-Mario Andretti

Why the Long Title?

- **Security** is paramount
- Consolidating **communication** and **collaboration** tools
- Shifting infrastructure from on-prem to the **cloud**

Outline

- What does Communication and Collaboration mean?
- How does security change as we move to the cloud?
- What are the risks?
- How do we protect data?
- How can cloud providers supporting detection and response?
- What are the key takeaways for us?
- What are we working on here at Penn?

Communication & Collaboration

Communication & Collaboration Technology

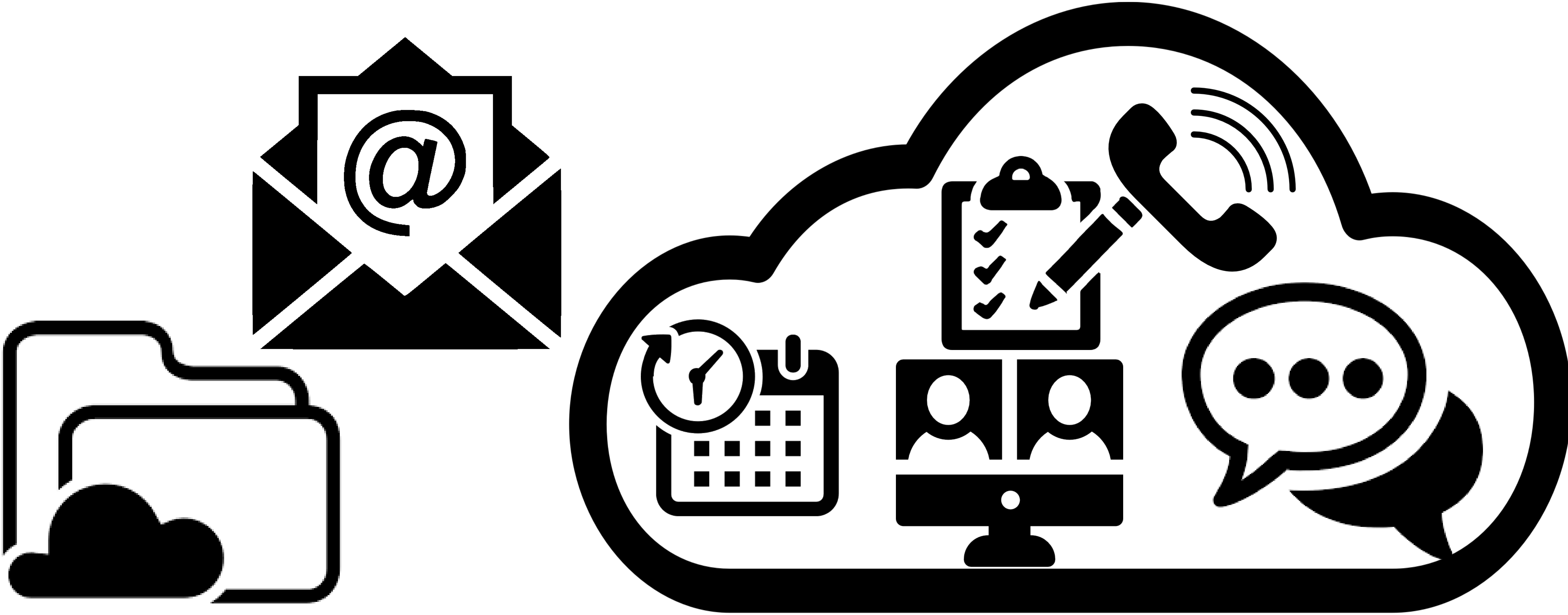
- Combination of distinct tools
- Tools often hosted on-prem
- Many different credentials for use

Communication & Collaboration Technology

Communication & Collaboration Technology

- Multipurpose tools
- Tools often cloud-based
- Fewer credentials across tools

Communication & Collaboration Technology



Exposure & Risk

Question: What are the risks?

- Tell me what you’re worried about!
- https://pollev.com/cmorganyoung189

What Are (Some of) the Risks?

- Credential Compromise (via Phishing/Spoofing)
- Data Breach
- Compromised bots/plug-ins/side-loaded apps
- System Vulnerabilities
- Denial of Service
- Humans
  - By error, lack of due diligence, or malicious intent

Data Exposure: What are we protecting?

- Sensitive, personal data
- Intellectual Property
- Reputation
- Trust

Example 1: Data Breach of 3rd Party Vendor

- Worst Case:
  - Data was unencrypted
  - Sensitive, personal data leaked
  - Same credentials used across multiple platforms

Example 2: Compromise via Phishing Email

- Worst Case:
  - Results in user providing credentials
  - Compromise goes undetected
  - Access to sensitive, confidential data
  - User access outside scope of employment
  - Compromise results in malicious use

Exposure & Risks: Takeaways

- Know what you’re protecting
- Cloud services: different risks, not fewer risks

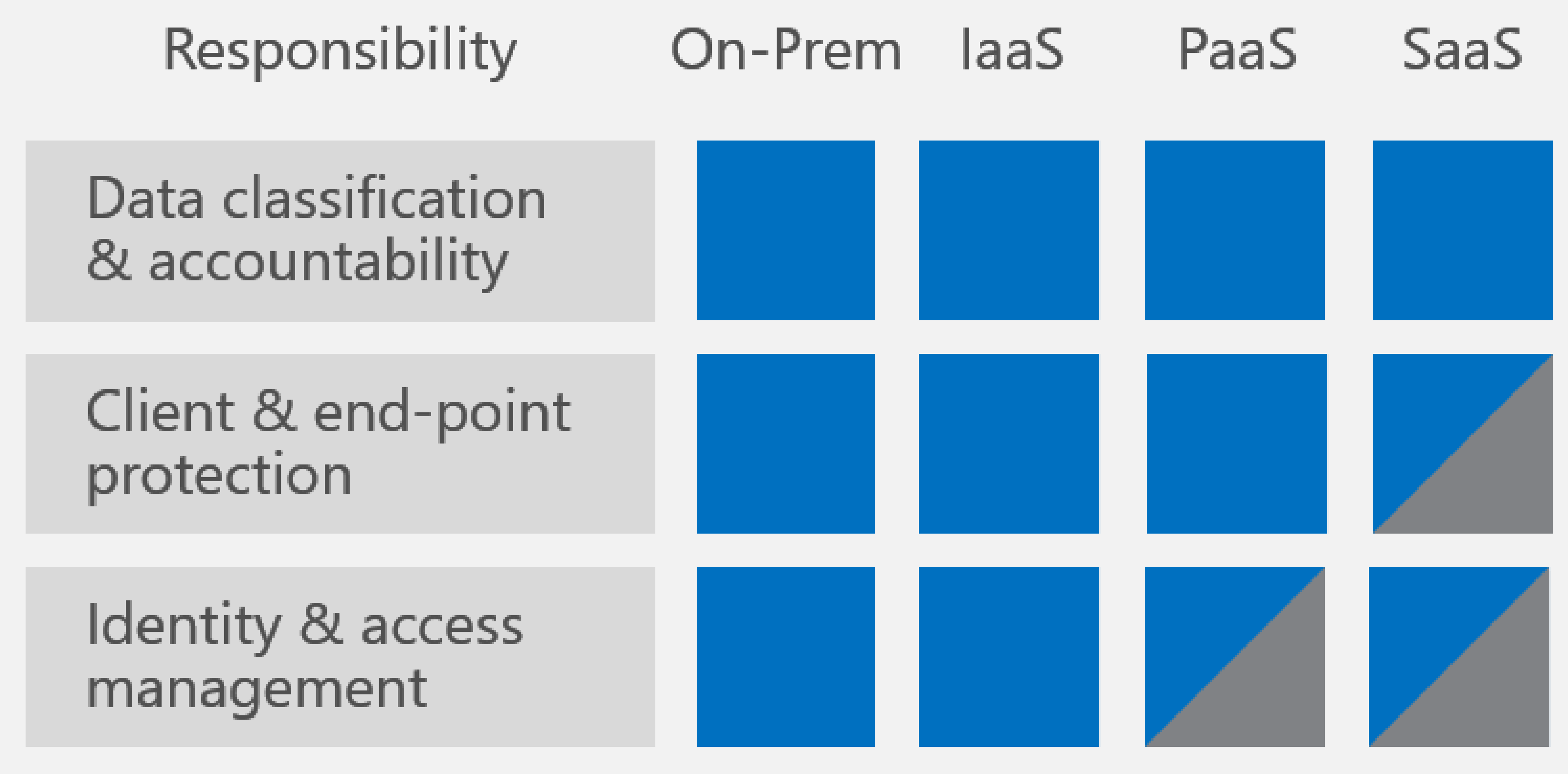
Protection & Prevention

Shared Responsibility Model

- How do our responsibilities change?
- Moving to cloud providers shifts responsibilities
- Obfuscation of on-prem security

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	🟦	🟦	🟦	🟦
Client & end-point protection	🟦	🟦	🟦	◩
Identity & access management	🟦	🟦	◩	◩
Application level controls	🟦	🟦	◩	⬛
Network controls	🟦	◩	⬛	⬛
Host infrastructure	🟦	◩	⬛	⬛
Physical security	🟦	⬛	⬛	⬛

🟦 Cloud Customer ⬛ Cloud Provider



Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	🟦	🟦	🟦	🟦
Client & end-point protection	🟦	🟦	🟦	◩
Identity & access management	🟦	🟦	◩	◩

Identity & Access Management

- Managing authentication is key
- Principle of Least Privilege:
  - Users have the minimum access needed
- Role-Based Access Control
- Multi-Factor/2-Step Authentication

Revisiting Example 2: Compromise via Phishing Email

- Previous Worst Case:
  - **Access to sensitive, confidential data**
  - **User access outside scope of employment**

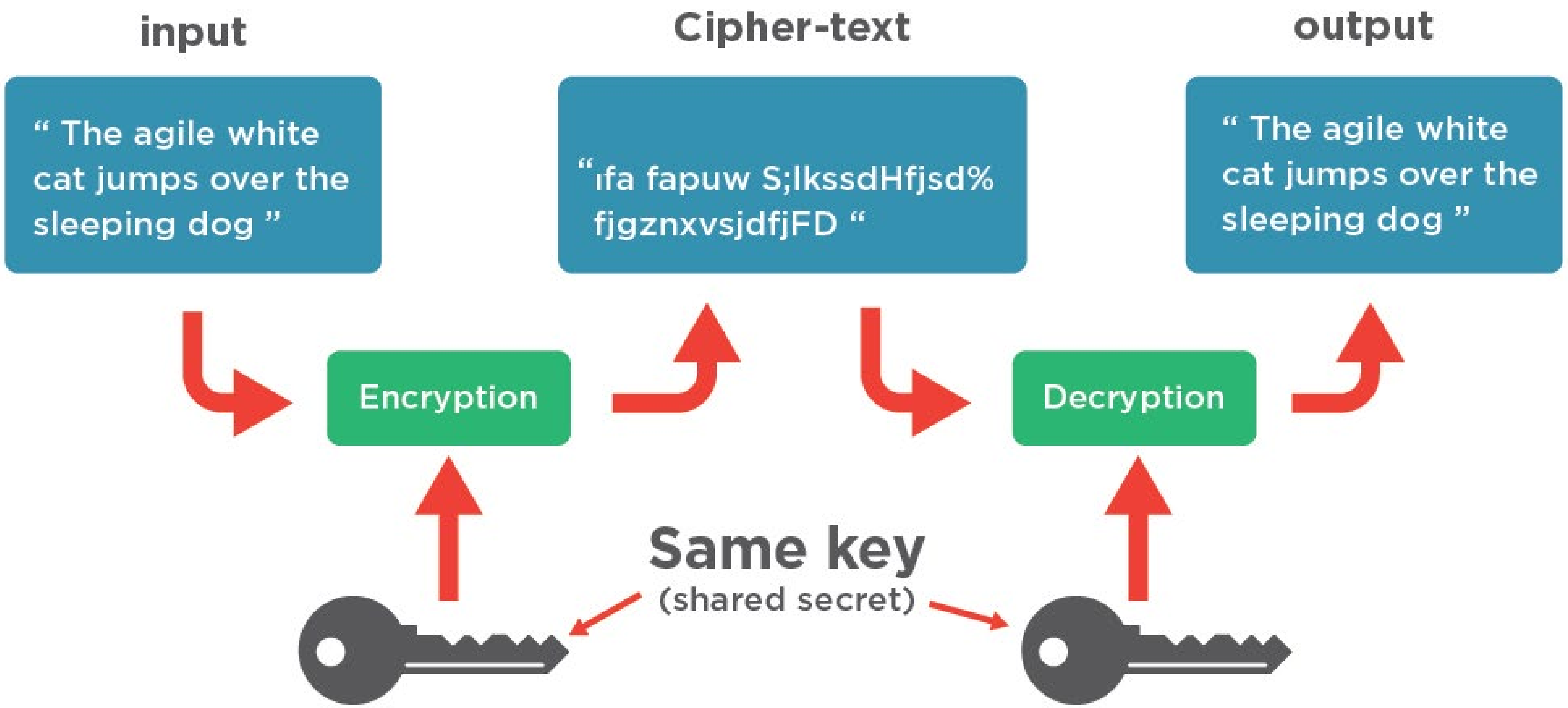
- With Principle of Least Privilege and RBAC:
  - Extent of compromised data is greatly reduced

- With Multi-Factor/2-Step Authentication:
  - Compromise may have been mitigated/avoided entirely

Data Security: Data at Rest

- Data is encrypted while not in use
  - Or: specific sensitive data is encrypted
- Use of strong, unique encryption keys
- Appropriate storage of keys

Data Security: Data at Rest



input

“ The agile white cat jumps over the sleeping dog ”

Cipher-text

“ıfa fapuw S;lkssdHfjsd% fjgznxvsjdfjFD “

output

“ The agile white cat jumps over the sleeping dog ”

Encryption

Decryption

Same key

(shared secret)

Data Security: Data at Rest

- On Penn Services:
  - Box
  - O365
  - Slack
  - SecureShare

- What About Personal Devices?
  - Mobility
  - Local Devices

Revisiting Example 1: Data Breach of 3rd Party Vendor

- Previous Worst Case:
  - **Data was unencrypted**

- With Encryption:
  - Data was encrypted
  - Effort to decrypt data is harder than it's worth

Data Security: Data in Transit

- Traffic over the internet
- Traffic between vendor data centers
- Email is a specific case

Data Security: Cloud Considerations

- No more perimeter
- Mobility and BYOD (Bring Your Own Device)
- Endpoint Protection is Key

Data Security: Takeaways

- We **share** responsibility for data protection
- **Encryption**, encryption, encryption!

Email Security & Penn’s Infrastructure

Email Security: Protocols

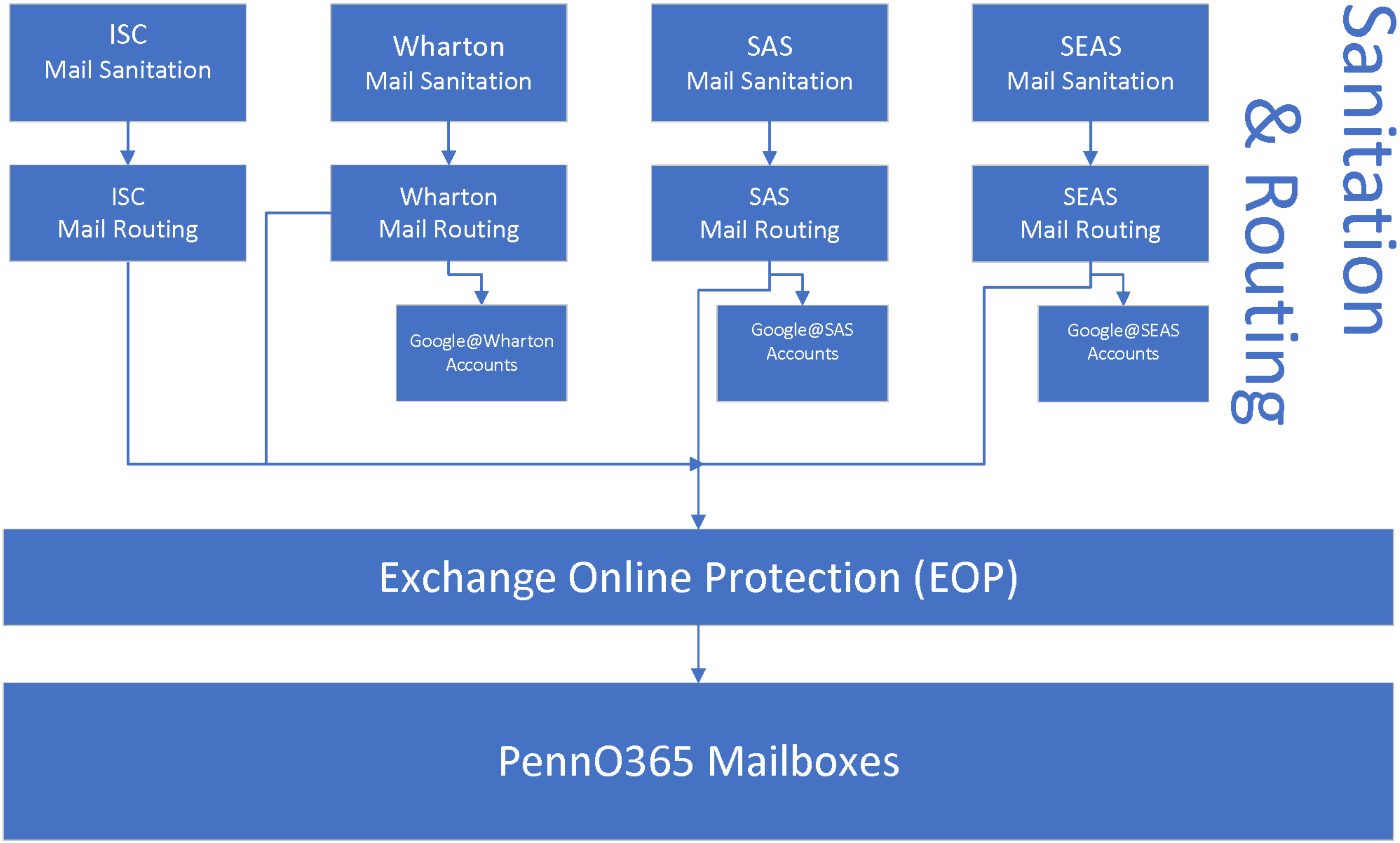
- TLS: Encrypting communication over a network
- SPF: Verifies if sender is allowed to send as a domain
- DKIM: Verifies email was sent by domain
- DMARC: Validates SPF & DKIM, validates sending addresses

Email Security Example 1: Spoofing, Phishing & Junk

- How does a Mail Sanitation Service know what's Junk?
  - Checks against implemented protocols, e.g. SPF and DKIM
  - Spam Heuristics

- Penn's sanitation and routing environment is decentralized

Sanitation & Routing



ISC Mail Sanitation

ISC Mail Routing

Wharton Mail Sanitation

Wharton Mail Routing

Google@Wharton Accounts

SAS Mail Sanitation

SAS Mail Routing

Google@SAS Accounts

SEAS Mail Sanitation

SEAS Mail Routing

Google@SEAS Accounts

Exchange Online Protection (EOP)

PennO365 Mailboxes

Revisiting Example 2: Compromise via Phishing Email

- Previous Worst Case:
  - Results in user providing credentials

- With Strong Email Security Protocols:
  - Phishing Email may have been blocked entirely, or moved to Spam

Email Security Example 2: False Positive Spam

- Failed protocol checks
- Heuristics Engine Detects:
  - Untrusted links
  - Untrusted attachments
  - Contents of the message (included attached or forwarded content)

Email Security Example 2: False Positive Spam

- Best Practices for Reporting False Positives:
  - Isolate triggers (attachments, links)
  - Original, non-forwarded messages are clearer
  - Submit most recent samples as attachments

Question: Sharing Sensitive Data

- The Admissions Department needs to share data about incoming students with the IT Department in order to create accounts. Once the accounts are created, IT doesn’t need the information anymore.

- What’s the best tool for this job? Why?

Email Security: Takeaways

- Security is determined by multiple protocols
- Heuristics grow and change

Detection & Response

Detection & Response

- Cloud Considerations:
  - Less reliance on Firewalls and local protections
  - More reliance on available tools of vendor
  - Vendors may have built-in baselines

Detection & Response

- Audit Logs
  - How to know what's not normal?
  - Know what logging is available to you
- Configuring Alerts
  - Constant, ongoing process

Revisiting Example 2: Compromise via Phishing Email

- Worst Case:
  - Compromise goes undetected
  - Access to sensitive, confidential data

- With Logging & Alerts set up:
  - Early notification of unusual behavior
  - Audit logs help identify what sensitive data may be exposed

Detection & Response: Takeaways

- Inventory: Know what's exposed
- IAM, RBAC: Better control of access can quicken response
- Be aware of what tools are available to help

Best Practices
& Future Improvements

Best Practices to Mitigate Risk

- Inventory: What, Where and How
- IAM & the Principle of Least Privilege
- Multi-Factor Authentication
- Vet Your Vendors (with V-STAR)
- User Education

Vet Your Vendors

- V-STAR
  - An offshoot of SPIA
  - Flexible tool to assess vendor security
- Asking the right questions can prepare you for issues that arise

User Education

- Communication is Key
- Build Relationships
- Emphasize the value of data

Recent Wins & Future Improvements

- 2-Factor Authentication for PennO365
- ProofPoint: Centralized Mail Routing & Security Enhancements
- Next Gen Unified Communications

Questions? Comments?

Cassandra Young { morc@isc.upenn.edu; }

Thanks to: security@isc, o365-tech@isc, stacc, harris2, sdriley, charlesr, sulm, sheminge,
sherrym, cathy, coco-tech, everyone I stopped in the hallway to bug!