IT Data Security in An MSO Environment

A Technical Paper Prepared for SCTE/ISBE by

Robert Gyori
Group Vice President
Information Technology, Security & Compliance
Charter Communications
13736 Riverport Dr.
St Louis MO. 63043
314-388-8820
Robert.gyori@charter.com

Table of Contents

List of Figures

List of Tables

Introduction

Are you in the process of launching a Security Program to support your Cable Company or are you looking to improve your existing program? This whitepaper and it's supporting presentation will help you get started. This document should help you identify what needs to be protected and some basic protection measures.

IT Data Security in an MSO Environment

This discussion will walk you through some of the basic questions you should consider if you are standing up a security program.

1. Do you know what types of data to protect and how to protect it?
2. What are your risk measurement criterion?
3. Are you using a standards based approach to secure your data and critical infrastructure?
4. How are you protecting and validating your compliance landscape?
5. How are you handling Identity Management?

This discussion will walk through some of the basic concepts around protecting critical data assets in our complex MSO networks…

What do you need to secure your data?

Answer: People, Process, & Technology…

With a solid foundation of polices/standards…

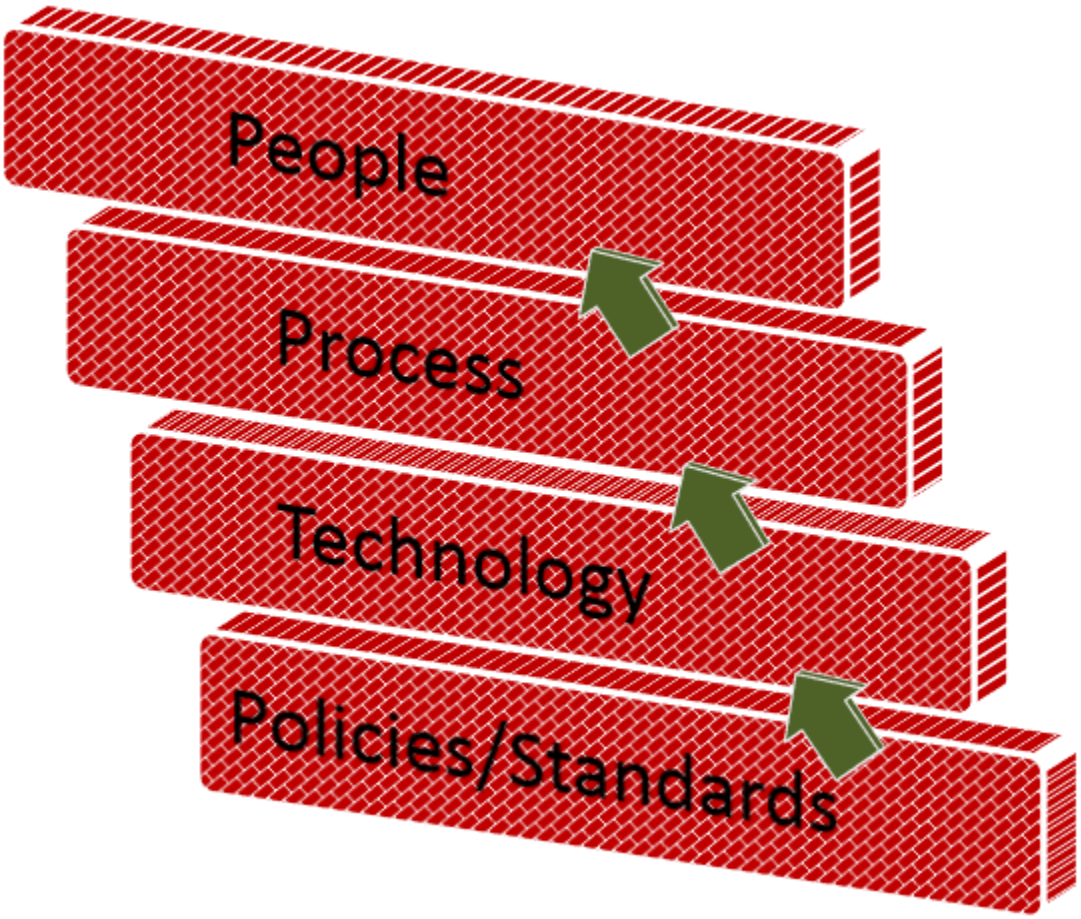

Figure 1 - People Process Technology

Take-away concept: These are foundational building blocks for securing your information…

The "Why"

Why do Cyber events happen in the MSO space?

What are the motives?

1. In the Service Provider Space
   1.1. Sample Event: DDOS Attacks against the backbone
   1.2. Anger
   1.3. Hacktivism
   1.4. An attempt to disrupt communications (internet access, news etc.)
   1.5. An attempt to penetrate laterally to the Crown Jewels…
2. In the IT and/or Enterprise Support Space
   2.1. Money is THE motice
   2.2. Sample Event: Corporate Financial Instrument theft, Customer/Employee PII/PCI/Sensitive Data (incl: CC)

Take-away concept: *Focus on items that lead to the most $ (lost or stolen)*

Discussion Point: *what is the half-life of PII?*

The "What"

What Cyber events can provide the most risk and/or impact to an MSO?

1. In the Service Provider Space
   1.1. Any interruption/degradation in the service we provide to our customers.
      1.1.1. E.g. DDOS Attacks against the backbone
   1.2. Any interruption/degradation in our ability to service our customers.
      1.2.1. Attacks against DNS, Customer Provisioning etc. (BACC/RDU etc.)
2. In the Enterprise Support Space
   2.1. Any Incident/Breach that impacted or resulted in the breach of :
      2.1.1. Corporate Financial Instruments
   2.2. E.g. Large scale unauthorized wire transfers etc.
      2.2.1. Customer PII/PCI/Sensitive Data
      2.2.2. Employee PII/PCI/Sensitive Data

Internal Vs. External: Background Stats…

1. Vast majority of threats (bad actors) resulting in incidents are external ~%75 (VZ 2016 & 2017 DBIR)
   1.1. Internal threats are important and DO exist….
      1.1.1. Internal threats have the potential to be devastating
      1.1.2. Internal threats can lead to or facilitate an incident from external threats
   1.2. Especially in orgs that are heavy in Intellectual Property or DoD based
2. Common thread in most incidents = Employee/Vendor Credentials (stolen and/or weak passwords)
   2.1. 63 % in 2016 (per Verizon 2016 DBIR)
   2.2. 81 % in 2017 (per Verizon 2017 DBIR)

Take-away concept: *So just how important is Identity/Credential Management to your security model?*

What Data Should you protect?

1. The Crown Jewels! Or… Soo much data so little time…
   1.1. MSO's store, process, and transmit data at all layers of their infrastructure. From STB data travelling upstream to billing and conditional access systems, to customer facing ".net" & eCom platforms.
   1.2. With so much data how do you know what should be the most protected?
   1.3. Or…What data would be the most valuable to a bad actor?
   1.4. Hint…Start with a Data Classification Policy applied to your data

   Take-away concept*: This is one of the many reasons that having sound polices is foundational….without a Data Classification Policy, it's hard to know what data is most valuable.*

How should you protect your data/systems?

1. Start with a standard based framework approach
   1.1. NIST Framework for Improving Critical Infrastructure Cyber Security
   1.2. NIST 800-53 Security & Privacy Controls
   1.3. ISO 27001/27002
   1.4. SANS Top 20
2. Write your polices/standards to map to your Framework
   2.1. Most of the controls from one framework can be mapped to the others
      2.1.1. For Example, SANS Critical Control #1:
         2.1.1.1. Inventory of Authorized & Unauthorized Devices
         2.1.1.2. Maps to > NIST 800-53 (CM-8, a,c,d,2,3,4 & PM 5, PM 6)
3. Implement your tools & develop your process based upon your framework
   1.1. Throw in some Capability Maturity Modelling (CMM) for leavening…

   Take-away concept**:** *Most standards have significant over-lap and can be cross-referenced etc.*

What about that Data Classification Policy?

Some Data Classification Samples: (Every company must define their own policy)

- **Public:** Information that does not fall within one of the more restrictive categories and that can be or has been made available to the public without any financial, legal or other implications to the Company
    - Examples (nonexclusive): Information in the public domain, on public websites, released press releases, published marketing materials, published annual reports, publically filed documents, etc.
- **Internal Only:** Information that is not Restricted or Sensitive and which is not approved for general circulation outside the company, where its disclosure would inconvenience the company, but is unlikely to result in significant financial loss or serious damage.
    - Examples (nonexclusive): internal memos, internal project reports, minutes of meetings, unreleased press releases, unpublished marketing materials, competitive analysis, internal non-proprietary policies, processes or procedures.
- **Restricted:** Information that is not Sensitive and which is considered critical to the organization's ongoing operations and could seriously impede or disrupt them if disclosed without authorization or made available to the public.
    - Examples (nonexclusive): accounting information, business plans, Personally Identifiable Information (PII) about customers or employees, etc.
- **Sensitive:** Any highly confidential internal information about customers or employees or other strategic or financial information which the loss of confidentiality, integrity, or availability could be expected to have an adverse effect on the company. The highest levels of integrity, confidentiality, and restricted availability are vital.
    - Examples (nonexclusive): customer or employee social security or tax identification numbers, driver's license or state issued identification numbers, financial or payment card information, impending mergers or acquisitions, investment strategies, etc.

Applying your Policy to specific use cases

Data Access Policy Sample for Storage

PHYSICAL STORAGE/ACCESS: defines how information may be stored when in a physical format. Inclusive of paper records and when electronic information is stored on a physical Medium (e.g., backup tapes, CDs, etc.).

Table 1 - Sample for Storage

Classification	Policy
Public	No Restrictions
Internal Only	• Protect from inadvertent or unauthorized disclosures • If physical media contains electronic data, then it also must be protected • Storage under lock and key • Only authorized users may have access
Restricted	• Access list must be reviewed periodically by business owner.
Sensitive	• Access to or removal of Information may only be granted with management approval. • Must be kept under double lock and key • Attempted or actual unauthorized access, use or disclosure must be immediately reportable to compliance teams • Appropriate entry controls must be used to limit and monitor physical access to areas containing physical media containing payment card data.

Data Access Policy Sample for Database Access

ELECTRONIC STORAGE/ACCESS: how information may be stored or accessed when in an electronic format (such as in a database)

Table 2 - Sample for Databases

Classification	Policy
Public	No Restrictions
Internal Only	• May be stored in unencrypted format. • Must have individual access controls where possible and appropriate. • Only authorized users may have access.

Restricted	• May be stored in unencrypted format.
	• Must have the following access controls:
	  • Must have individual access controls that restrict access to active Users and active User account only
	  • Must assign unique IDs and passwords, which are not vendor supplied defaults, to each Users
	  • When being accessing via a public network, logon credentials may not be passed in clear text
	• Access list must be reviewed periodically by the business owner.

Data Access Policy Sample for Database Access (Continued)

Classification	Policy

Sensitive	• Information must be encrypted
	• Must have the following access controls:
	  • Individual access controls that restrict access to active User account only
	  • Restrict access to those who need information to perform their legitimate job duties
	  • Block access to any User ID after multiple unsuccessful attempts to gain access
	  • Assign unique IDs and passwords, which are not vendor supplied defaults, to each user
	  • When being accessing via a public network, logon credentials may not be passed in clear text
	  • Access must be logged for a minimum of 30 days.
	• Access list must be reviewed on a quarterly basis by business owner.
	• Attempted or actual unauthorized access, use or disclosure must be immediately reported.
	• Within the Payment Card Industry (PCI) payment card environment, users, system administrators, and vendors accessing systems that store data classified as restricted or sensitive from outside the network must use additional criteria for authentication.
	• Such criteria are commonly referred to as "two factor authentication".
	  • Something you know, such as a password or passphrase
	  • Something you have, such as a token device or smart card
	  • Something you are, such as a biometric
	• For systems within the PCI payment card environment, only authorized users may query databases directly.
	• Standard user accounts must not have the ability to directly query databases that house sensitive or restricted data.

Policy Sample for Data Retention How long data is retained in its readable state before being subject to deletion or destruction. Data Retention is not defined by classification or categorization. Data retention policies are defined case-by-case for data stored in a database for the purposes of the application. The retention policy is defined to be greater than the legal minimum and the lesser of:

1. *Legal maximum data retention requirement*
2. *Application requirement to have the data available*

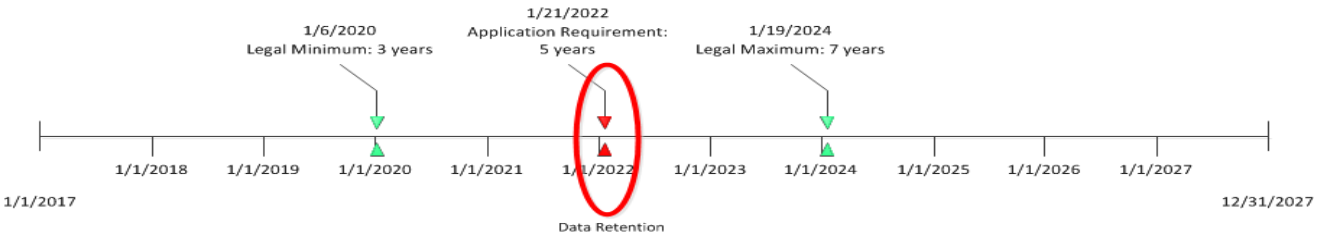

Figure 2 Data Retention 1

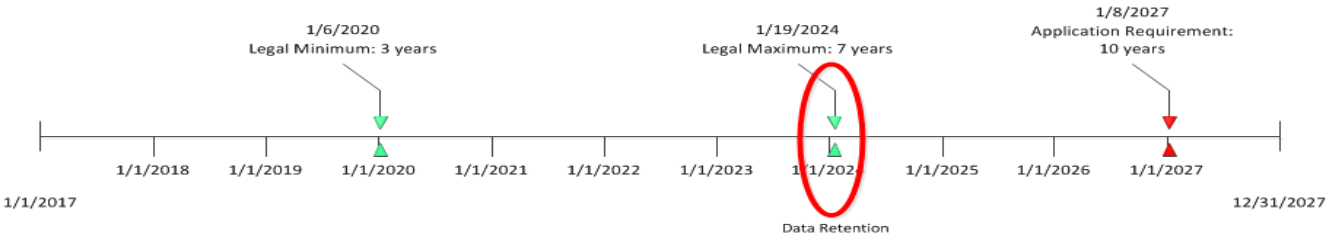

Figure 3 - Data Retention 2

Table 3 - Data Retention

Group	Responsible for
Legal	Definition of the data retention policy for the data in question
Application Owner	Non-functional requirements pertaining to the retention of data
System Administrator	Enforcement, monitoring, and reporting of the data retention policy

Policy Sample for Data Disposal/Destruction

Table 4 - Data Disposal

Classification	Policy
Public	No Restrictions
Internal Only	Electronic data must be erased or rendered most likely unreadable.
Restricted	Electronic data must be completely erased or rendered difficult to retrieve.
Sensitive	Electronic data must be completely erased and overwritten or rendered reasonably unrecoverable.

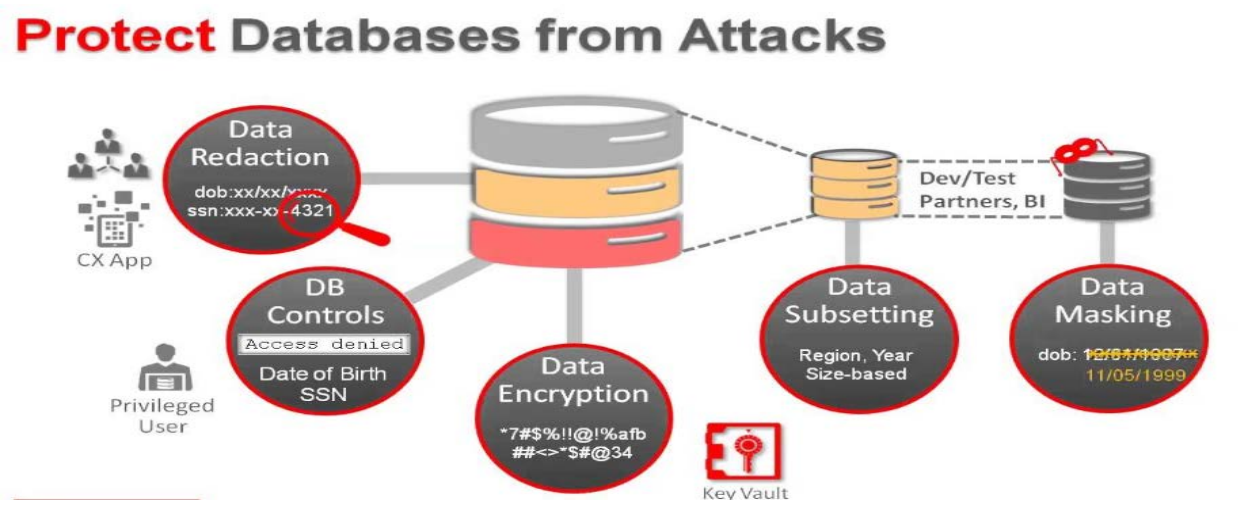

Figure 4 - Database Protection

Protecting databases from attacks

Sample Data Protection Policies/Standards

Table 5 - Data Protection

Technology	Description	Platform(s)
Encrypted Database	All files in the DMBS (database management system) are encrypted with keys known only to the administrators. If the database is separated from the application or the installation, the data is unrenderable	Oracle, MSSQL, MySQL, Teradata
Encrypted Tablespace	All tables in a defined tablespace are encrypted with keys known only to the administrators. If the data in the table is separated from the tablespace, the data in unrenderable	Oracle, MSSQL, MySQL, Teradata
Encrypted Column	All data in a defined column of a table is encrypted with keys known only to the administrators. If the data in the columns is separated from the table, the data in unrenderable	Oracle, MSSQL, MySQL, Teradata
Key Vaults	Repository with encryption keys for real-time data access via certificate, used to unencrypt data for use. This prevents applications from having native keys.	All
Access Controls and Role based privileges	Logins with defined permissions for data access. Roles are by default "deny all" and permissions to view data in databases must be ***added***.	All
Encrypted Storage	Encryption of the data at rest in the storage servers. This is storage technology, not database technology, but applies to many of the databases in a N-tier architecture (where compute is separate from storage). Encryption of the stored data at-rest renders data unreadable without the separately stored keys.	EMC, Hitachi, NetApp, Violin

Sample Practices to implement Data Protection Policies/Standards

Table 6 - Data Protection Practices

Preventative	Detective	Administrative
Encryption Using technology to cypher data in such a way that it cannot be rendered without the cypher keys	**Monitoring** Using technology to monitor behaviors of data users, and alerting administrators of abnormalities	**Governance** Tracking and cataloging of data access granted to users. Regular audits of users and applications
Data separation The practice of storing partial data sets in separate data stores, resulting in the need for multiple data breaches in order to lose meaningful data	**Firewalls** Devices with abilities to detect abnormal traffic to and from data stores (databases and storage)	**Key Management** Storing the keys for encrypted data separate from the data or application. This practice essentially means you have to steal the database and the DBA to compromise the data.
Data classification Defined classifications for data sets for the purposes of defining the appropriate data protection level	**Human Intelligence** Anonymous portal for solicitation and documentation of events with potential security ramifications	**User Management** Enforcement of best practices for password rotation and complexity
User Controls Minimalist approach to data access. Individual users for every person or application with legitimate data access needs. Pre-defined roles for categories of users. Regular rotation of passwords.		**Configuration** Patching and upgrades of environments to prevent data compromise

Layered Security along the path…Protecting Data in Motion

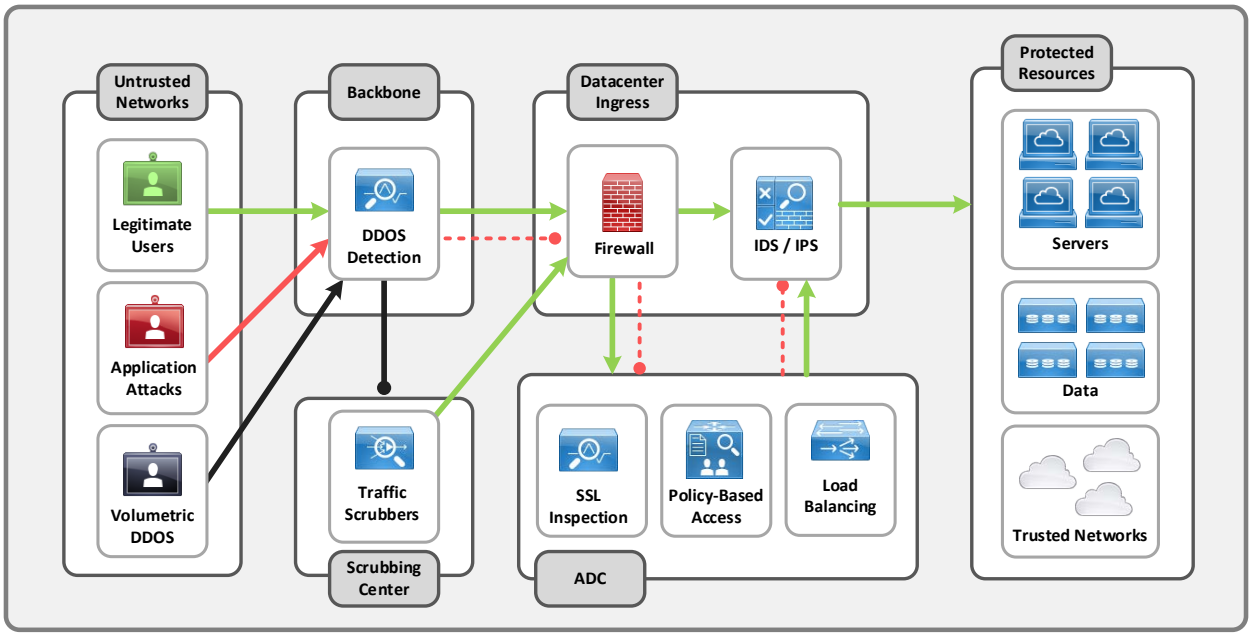

Figure 5 - Layered Security

Threat Prevention & Mitigation Sample Tools

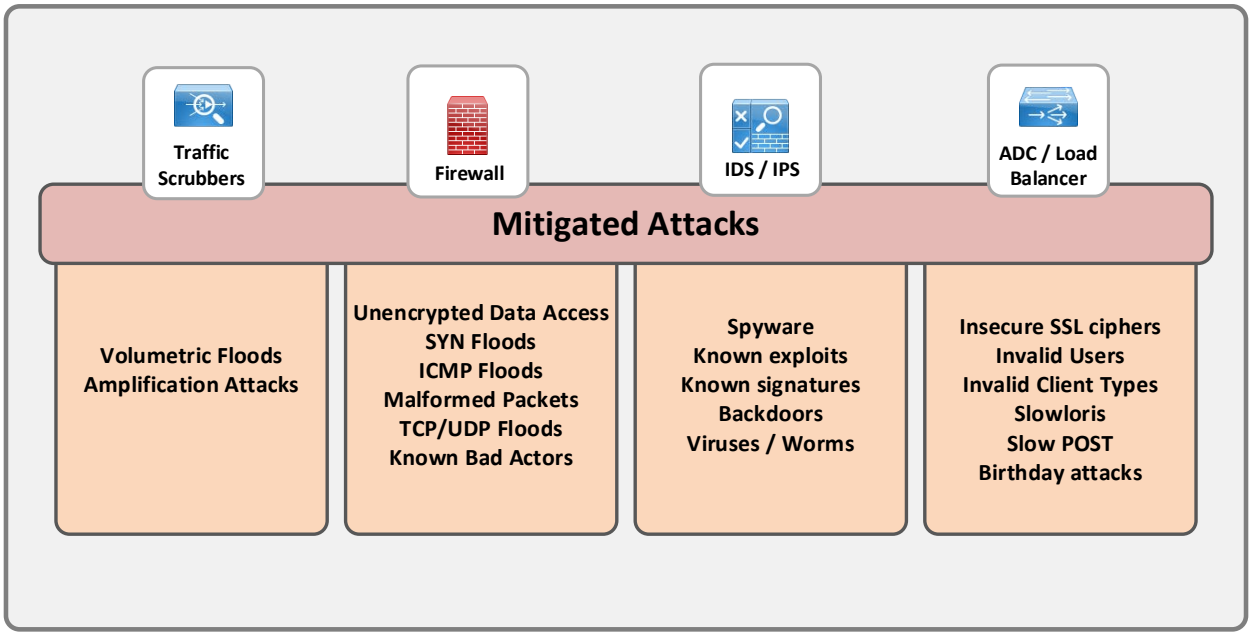

Figure 6 - Threat Prevention & Mitigation

Using Protocol Discretion

Table 7 - Protocol Discretion

Usage	Insecure Protocols (prohibited)	Secure Protocols (allowed)
Web Services	HTTP, SSL, TLS1.0	HTTPS, TLS1.2/1.1
File Transfer	FTP, RCP	SFTP, SCP
Remote Shell	Telnet, SSH1	SSH2
Remote Desktop	VNC	RDP

Compliance Obligations

Sectoral Approach to Privacy and Data Security in the U.S.

1. Sector-specific federal legislation (financial services, health care, and education) and marketing restrictions.
2. State laws fill gaps or raise standards (e.g., consumer privacy, breach notification, and data security).
   2.1. E.g., State information security laws requiring "reasonable" security (i.e., Massachusetts information security regulations).
   2.2. Secure data disposal and SSN protection laws.
3. Industry standards, voluntary codes, and government guidance also play key role.
4. Various state and federal agencies enforcing privacy and data security laws and regulations, including the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), etc.

   Sometimes Compliance Obligations may drive your security program

In our regulated business, compliance is usually not an option…

1. Sarbanes-Oxley Act of 2002 (SOX)

2. Health Insurance Portability and Accountability (HIPAA) and Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)
3. Customer Proprietary Network Information (CPNI)
4. Payment Card Industry (PCI)

SOX

Sarbanes Oxley

1. Focus on strengthening financial reporting in publicly-traded companies in response to large-scale financial scandals, such as Enron & WorldCom.
2. Provides corporate governance guidelines for companies, their boards, and their auditors.
   2.1. Does not explicitly mention data security issues; however, the auditing standards emphasize that upper-level management is responsible for ensuring the integrity of controls on data privacy and security.
   2.2. Controls on data stored with 3rd parties significant part of a SOX-compliant audit report

HIPAA / HITECH

Health Insurance Portability and Accountability
Health Information Technology for Economic & Clinical Health

Protecting Employee data

1. Together, HIPAA and HITECH require implementation of data security requirements to protect the privacy and security of "protected health information" (PHI).
2. HIPAA's information security requirements apply to "covered entities" (i.e., health plans and healthcare providers), and HITECH's amendments expanded application to "business associates" that perform business services for the covered entity.
3. HIPAA also requires that covered entities conduct a security risk analysis to assess the potential risks and vulnerabilities of all electronic PHI created, received, maintained, or transmitted.
4. Need coordination between IT/NetOps etc. (employee data vs customer data)

CPNI

Customer Proprietary Network Information

1. The Federal Communications Commission (FCC) imposes detailed regulations that limit access, use and disclosure of CPNI in the context of voice services.
   1.1. CPNI is certain types of information (i.e., subscription information, call detail records, etc.) collected by telecommunications carriers related to their subscribers.
2. The CPNI regulations require carriers to take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI including:
   2.1. The use of proper account authentication; and providing notification to customers when certain account information activity occurs (i.e., after a customer's password, security question and answer, online account, or address of record is created or changed).
   2.2. Rules for CPNI in the ISP are still not finalized. Per FCC guidance MSO's should exercise reasonable good faith efforts to comply with the general nature of CPNI rules.

PCI

Payment Card Industry

1. PCI Data Security Standard (DSS) first took effect in June 2005; current version 3.2 came into effect in April 2016
   1.1. Requires merchants and credit card transaction processors that store, process or transmit cardholder data to build and maintain a secure computer network, maintain a vulnerability management program, and regularly monitor and test networks.
   1.2. The technical/operational requirements include restricting access to data, encrypting sensitive data transmitted over public networks, the use of firewalls, current virus software, and other data security measures.
   1.3. The requirements extend to application development and security processes to ensure PCI is protected throughout the applications lifecycle
2. Note that some states (e.g., Nevada and Washington) have codified compliance with PCI DSS requirements into state statutes.
3. In Scope vs. Out of Scope

3.1. Category 1 = Systems that Transmit, Process, Store Credit Card Data
3.2. Category 2 = Systems connected to Cat 1
3.3. Concept of "infected"

4. Drives businesses to improve security
5. Drives business to improve security specific to In Scope systems
5.1. Build & Maintain a Secure Network & Systems
5.2. Protect Cardholder Data
5.3. Maintain a Vulnerability Management Program
5.4. Implement Strong Access Control Measure
5.5. Monitor and Test Networks
5.6. Maintain an Info Sec policy.
6. PCI drives concepts that should already be in place in a mature security program
6.1. Logging
6.2. Change/Configuration management
6.3. Encryption
6.4. Patch & Vulnerability Management

Do you want to limit your systems considered in-Scope for PCI?

1. Don't: Transmit/Process/Store Cardholder Data!
1.1. This actually does have some merit…
2. Network Segmentation
2.1. Not a PCI requirement BUT does help reduce scope
3. Tokenization
3.1. Replace any CC data in transit with tokens

Reducing your PCI scoped systems, can reduce your PCI cycles/costs

Identity Management & Access Control

1. It's difficult to extract/steal sensitive data without a legitimate credential…
2. Going back to the stats:
3. Common thread in most incidents = Credentials (stolen and/or weak passwords)
3.1. 63 % in 2016 (per Verizon 2016 DBIR)

3.2. 81 % in 2017 (per Verizon 2017 DBIR)

4. Password Fatigue: Users have to maintain credentials for multiple systems.
   4.1. Show of hands….
   4.2. Enterprise Single Sign-On (ESSO) helps reduce Password Fatigue BUT makes it even more critical that your identity management/credential management system is rock solid.
      4.2.1. But with ESSO a single stolen password could be used to access multiple systems…
5. Implement/Upgrade your Identity Management Systems
6. Consider a dedicated IDM not keyed to an email account
   6.1. Many enterprises only use Active Directory…
   6.2. Multiple vendors in the identity management space
7. Use IDM as the source of truth instead of HR Systems
   7.1. Place IDM at the center and feed other systems
   7.2. Your unique ID should never change or be reused
8. Manage/Model your IDM Lifecycle
   8.1. Identities may start with an HR or Recruiting system
9. Upgrade your Active Directory footprint
   9.1. Red Forest etc.

How much does a breach cost?

Table 8 - Cost of a Breach

	Anthem (Source: Cnet)	Home Depot (Source: Fortune)	Target (Source: Target)
Damages	$115,000,000	$ 179,000,000	$202,000,000
Customers/Records	80,000,000	50,000,000	40,000,000
Cost per/Record (Calculated)	$ 1.44	$ 3.58	$ 5.05

Conclusion

Maintaining secure systems and staying compliant in a MSO environment requires a multi-faceted cross-functional approach. Active collaboration between Information Technology, Network Operations/Engineering, and Legal is critical to the success of a security program. It should also be stressed again that the approach needs to contain a good mix of People, Process, Technology, and Policies/Standards.

Abbreviations

CC	credit card
CPNI	Customer Proprietary Network Information
DBIR	Data Breach Investigations Report
DDOS	distributed denial of service
ESSO	Enterprise Single Sign-On
FCC	Federal Communications Commission
FTC	Federal Trade Commission
HIPAA	Health Insurance Portability and Accountability
HITECH	Health Information Technology for Economic & Clinical Health
ISO	International Standards Organization
NIST	National Institute of Standards & Technology
PII	personally identifiable information
PCI	Payment Card Industry

SCTE	Society of Cable Telecommunications Engineers

Bibliography & References

NIST 800-53 Rev. : National Institute of Standards & Technology, Security and Privacy Controls for Federal Information Systems and Organizations

NIST Framework for Improving Critical Infrastructure for Cybersecurity, Version 1.0

PCI DSS 3.2: Payment Card Industry Data Security Standard, Version 3.2

