

Managing Identity and Authentication

- User Authentication is the starting point for effective identity management
- Two-factor authentication to verify user identity
- Adaptive Authentication

What Matters Most?

Risk Management

- Securing Data
- Managing Access
- Securing Systems and Networks
- Managing Identity and Authentication

User Awareness

- Managing User Awareness
- Securing Users
- Enforcing Compliance

People

How do you control what is out of your control?

- Expected behaviors
- Notifications and reporting
- Effective policies
- Training & Awareness



Mobile Forensics and Auditing

Discovering Risks and Building Solutions for BYOD / BYOE in Your Environment

Presented by:
Matt Malone



Managing Access

Well-defined role-based access

- Reliable process
- Assignment of roles and permissions
- Contingent on role vs. individual
- Oversight
- Functional system to modify access



Ensuring Users & Enforcing Compliance

- Mandatory security training
- Test effectiveness and compliance
- Detect and correct controls



About the Presenter:

Mr. Malone has over 15 years of proven experience within the information security realm. He has assisted customers post incident, working with national consulting firms to reduce or eliminate fines levied against his clients. Mr. Malone consults with the FBI on security threats and attacks, assisting with investigations, documentation and pursuit of offenders. Mr. Malone has gained valuable experience working with enterprise organizations and governmental agencies and serves on several advisory boards. Security source for FOX news as it relates to information security as well as incident response.

BYOD IS HERE



12:00

Securing Systems and Networks

- Risk based, comprehensive skills
- System and log monitoring
- Network penetration tests to detect malicious activities
- Risk reduction and patch software patching



Recommendations

Risk Management

- Secure data, not devices
- Risk Assessment and Mitigation
- Build and deploy system architecture
- Security and Compliance

User Management

- Risk based, comprehensive skills
- System and log monitoring
- Network penetration tests to detect malicious activities
- Risk reduction and patch software patching

Incident Response

- Plan for the worst, hope for the best
- Develop an incident response plan for critical business data

QUESTIONS?

Matt Malone
matt.malone@slaitconsulting.com
PH: 512-466-0179



User Awareness and Enforcement

- User behavior
- Even the most intelligent users make mistakes
- User understanding of security practices vs. actual compliance
- Good policies do not always translate to good security
- Test your policies



Mobile Forensics and Auditing

Discovering Risks and Building Solutions
for BYOD / BYOE in Your Environment

Presented by:
Matt Malone



About the Presenter:

Mr. Malone has over 15 years of proven experience within the information security realm. He has assisted customers post incident working with national acquiring banks to reduce or eliminate fines levied against his clients. Mr. Malone consults with the FBI on security threats and attacks, assisting with investigation, documentation and pursuit of offenders. Mr. Malone has gained valuable experience working with enterprise corporations and governmental agencies and serves on several advisory boards. Security source for FOX news as is relates to information security as well as incident response.

BYOD IS HERE

Accessing data from their personal devices

- Notes and Memo's
- Access to Email
- Passwords and credentials stored
- Pictures (White board, IDF's)



12:00

Tuesday, June 18

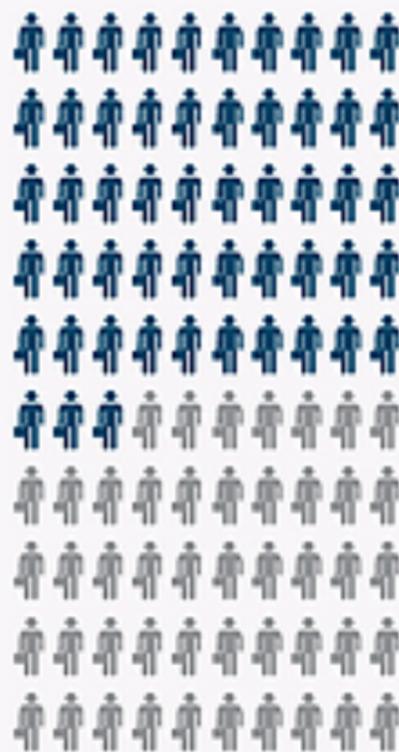


THE RISE



3 out of 4

professionals use **personal devices** to access **corporate data**



53%

of employees bring a **personal device** to work



of organizations expect a **2x - 10x increase** in BYOD devices in 2 years

THE RISK



out of the
70 MILLION devices
lost or stolen each year
ONLY 7% recovered



43% mobile devices that are
not password protected



65% companies that **cannot**
wipe devices remotely



76% companies that **do not**
encrypt mobile devices

THE RESULT



60%

network breaches **due to a lost or stolen device**



50%

companies that experienced a **data/security breach because of BYOD**

\$7.2 MILLION

average cost of single corporate **data breach**

What Matters Most?

Risk Management

- Securing Data
- Managing Access
- Securing Systems and Networks
- Managing Identity and Authentication

User Awareness

- Raising User Awareness
- Educating Users
- Enforcing Compliance

Securing Data

- Securing data, not devices
- One size never fits all
- Assessment and design critical to implementation of Best Practices
- Data should reside on secure servers
 - Encrypted at rest and in transit
 - View-only of critical data

Managing Access

Well-defined role-based access

- Reliable process
- Assignment of roles and permissions
- Contingent on role vs. individual
- Oversight
- Functional system to modify access



Managing Identity and Authentication

- User Authentication is the starting point for effective identity management
- Two-factor authentication to verify user identity
- Adaptive Authentication

People

How do you control what is out of your control?

- Expected behaviors
- Notifications and reporting
- Effective policies
- Training & Awareness



ness
awareness
s
pliance

User Awareness and Enforcement

User behavior

- Even the most intelligent users make mistakes

User understanding of security practices vs. actual compliance

- Good policies do not always translate to good security
- Test your policies



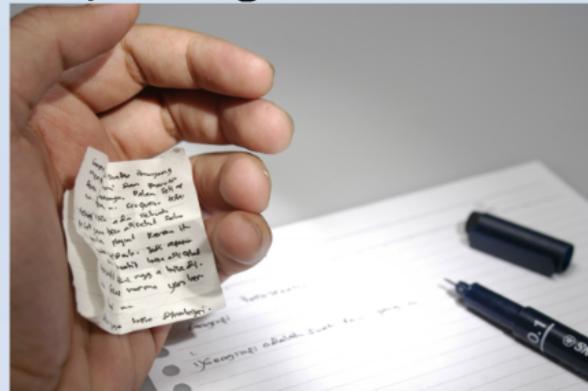
Educating Users & Enforcing Compliance

- Mandatory security training
- Test effectiveness and compliance
- Detect and correct controls



Securing Systems and Networks

- Routine and comprehensive audits
- System and log monitoring
- Network penetration tests to detect malicious outsiders
- Find problems not pass without findings



Recommendations

Risk Management

- Secure data, not devices
- Role-based access and oversight
- Routine and frequent system and network audits

User Management

- Two-factor authentication to verify user identity
- Educate users about security concerns
- BYOE security policies in place and easily accessible
- Monitor and enforce compliance

Incident Response

- Plan for the worst hope for the best
- Develop an incident response plan for mobile device disclosure

QUESTIONS?

Matt Malone
matt.malone@slaitconsulting.com
Ph: 512-650-0179



Managing Identity and Authentication

- User Authentication is the starting point for effective identity management
- Two-factor authentication to verify user identity
- Adaptive Authentication

What Matters Most?

Risk Management

- Securing Data
- Managing Access
- Securing Systems and Networks
- Managing Identity and Authentication

User Awareness

- Managing User Awareness
- Securing Users
- Enforcing Compliance

People

How do you control what is out of your control?

- Expected behaviors
- Notifications and reporting
- Effective policies
- Training & Awareness



Mobile Forensics and Auditing

Discovering Risks and Building Solutions for BYOD / BYOE in Your Environment

Presented by:
Matt Malone



Managing Access

Well-defined role-based access

- Reliable process
- Assignment of roles and permissions
- Contingent on role vs. individual
- Oversight
- Functional system to modify access



Ensuring Users & Enforcing Compliance

- Mandatory security training
- Test effectiveness and compliance
- Detect and correct controls



About the Presenter:

Mr. Malone has over 15 years of proven experience within the information security realm. He has assisted customers post incident, working with national consulting firms to reduce or eliminate fines levied against his clients. Mr. Malone consults with the FBI on security threats and attacks, assisting with investigations, documentation and pursuit of offenders. Mr. Malone has gained valuable experience working with enterprise organizations and governmental agencies and serves on several advisory boards. Security source for FOX news as it relates to information security as well as incident response.

BYOD IS HERE



Securing Systems and Networks

- Risk based, comprehensive skills
- System and log monitoring
- Network penetration tests to detect malicious activities
- Risk reduction and patch software patching



Recommendations

Risk Management

- Secure data, not devices
- Risk Assessment and Mitigation
- Build and deploy system architecture
- Audit and monitor user activities

User Management

- User Awareness and Training
- Role-based access control (RBAC) systems
- RBAC on all systems to enforce security
- Enforce and monitor compliance

Incident Response

- Plan for the worst, hope for the best
- Develop an incident response plan for critical business data

QUESTIONS?

Matt Malone
matt.malone@slaitconsulting.com
PH: 512-466-0179



User Awareness and Enforcement

- User behavior
- Even the most intelligent users make mistakes
- User understanding of security practices vs. actual compliance
- Good policies do not always translate to good security
- Test your policies



12:00