

# **CSX – Cybersecurity Fundamentals**

## **Section 6 : Security Implications and Adoption of Evolving Technology**



# Course Plan

Module Titles
Section 1 – Cybersecurity Introduction and Overview
Section 2 – Domain 1: Cybersecurity Concepts
Section 3 – Domain 2: Security Architecture Principles
Section 4 – Domain 3: Security of Networks, Systems, Applications and Data
Section 5 – Domain 4: Incident Response
Section 6 – Domain 5: Security Implications and Adoption of Evolving Technology
Section 7 – Course Review
Section 8 – Practice Exam



# Learning Outcomes for this Module

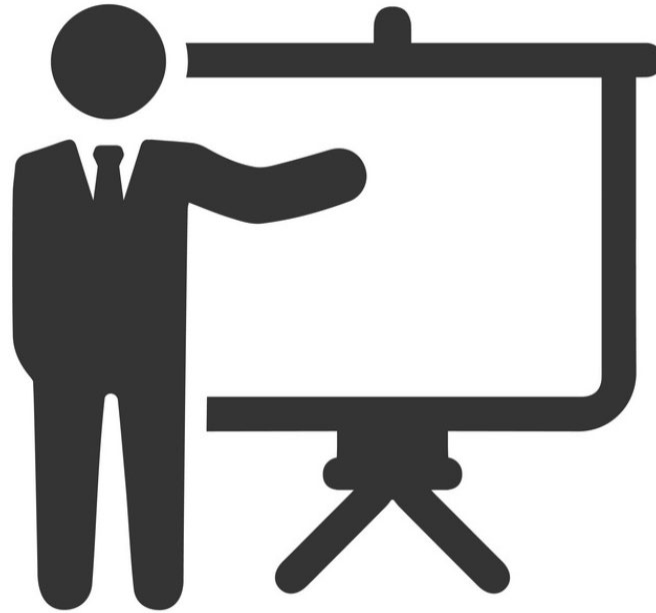
- Knowledge of emerging technology and associated security issues, risk and vulnerabilities
- Knowledge of risk associated with mobile computing
- Knowledge of cloud concepts around data and collaboration
- Knowledge of risk of moving applications and infrastructure to the cloud
- Knowledge of risk associated with outsourcing
- Knowledge of supply chain risk management processes and practices



## Topics for this Module

- **6.1** Current threat landscape
- **6.2** Advanced persistent threats (APTs)
- **6.3** Mobile technology – vulnerabilities, threats and risks
- **6.4** Consumerization of IT and mobile devices
- **6.5** Cloud and digital collaboration

# Current Events



Section 6.1

**Current threat landscape**

# Current threat landscape

- European Union Agency for Network and Information Security (ENISA)

- 2018 Report 

## Motivation:


- Financial gain
- Intellectual property
- Politics

1. Malware	↑	→
2. Web based attacks	↑	→
3. Web application attacks	↑	→
4. Denial of service	↑	↑
5. Botnets	↑	↓
6. Phishing	→	↑
7. Spam	↓	↑
8. Ransomware	→	↑
9. Insider threat (malicious, accidental)	→	↓
10. Physical manipulation/damage/theft/loss	↑	↓
11. Exploit kits	↑	↓
12. Data breaches	↑	↓
13. Identity theft	↓	↓
14. Information leakage	↑	↓
15. Cyber espionage	↓	→

### Trends:

Increasing 

Stable 

Decreasing 

### Ranking:

Going up 

Same 

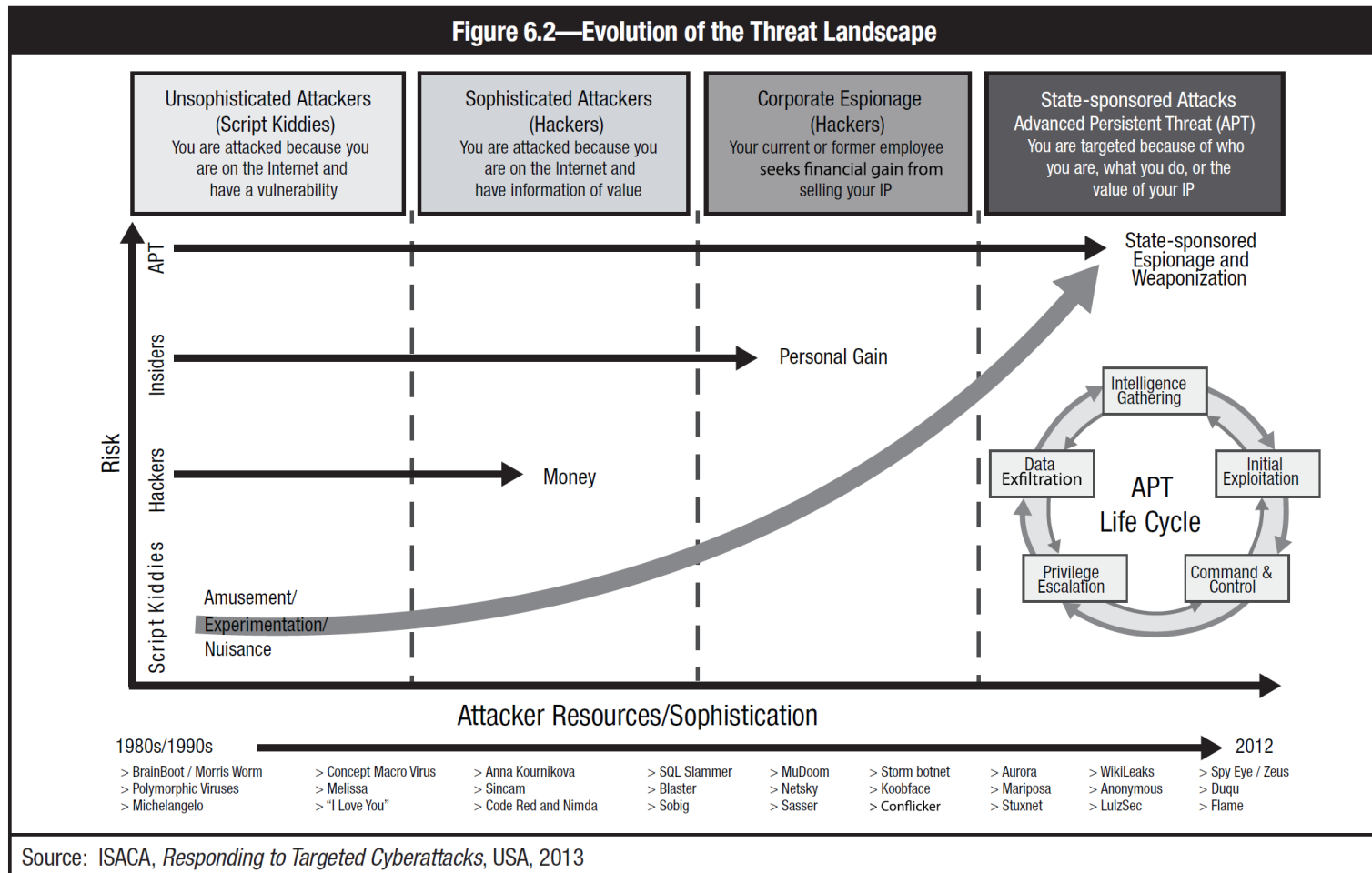
Going down 

Section 6.2

**Advanced persistent threats**



# Advanced persistent threats



**APT Definition :** is a targeted threat that is composed of various complex attack vectors and can remain undetected for an extended period of time.



# APT introduction Video

THREAT



HUMAN  
INVOLVEMENT  
ORCHESTRATING  
ATTACK

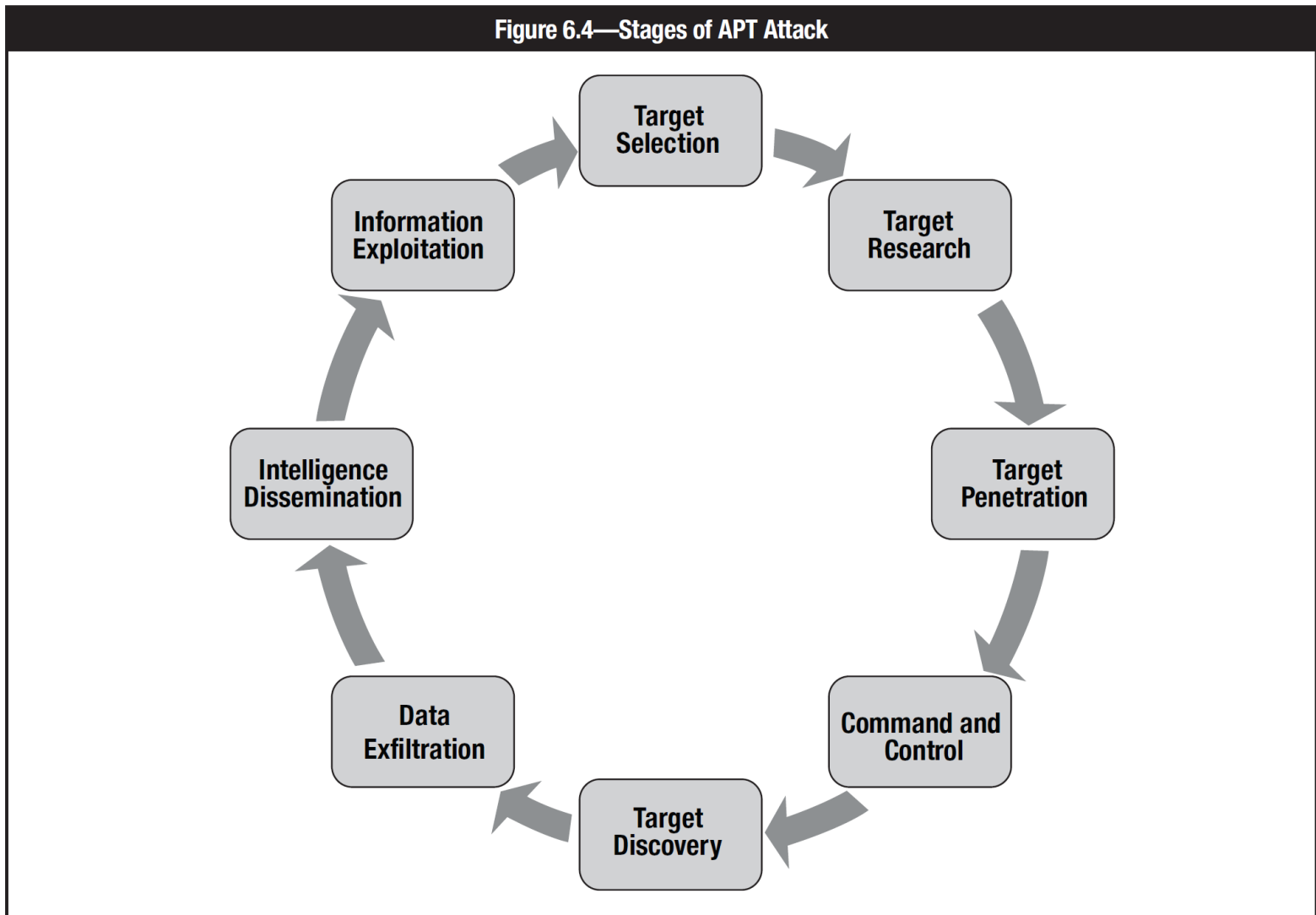
Link: <https://www.youtube.com/watch?v=DsV2XRQKrcs>



# APT characteristics

- **Well-researched**—APT agents thoroughly **research their targets**, plan their use of resources and anticipate countermeasures.
- **Sophisticated**—APT attacks are often designed to exploit multiple vulnerabilities in a single attack. They employ an **extensive framework** of attack modules designed for executing automated tasks and targeting multiple platforms.
- **Stealthy**—APT attacks often **go undetected** for months and sometimes years. They are unannounced and disguise themselves using obfuscation techniques or hide in out-of-reach places.
- **Persistent**—APT attacks are **long-term projects** with a focus on reconnaissance. If one attack is successfully blocked, the perpetrators respond with new attacks. Plus, they are always looking for methods or information to launch future attacks.

# Stages of an APT attack



**Any questions?**

Section 6.3

**Mobile technology – vulnerabilities,  
threats and risk**

# Mobile application

- OWASP – Mobile top 10 critical mobile security flaws - 2016

## **M1 - Improper Platform Usage**

This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk.

## **M2 - Insecure Data Storage**

This new category is a combination of M2 + M4 from Mobile Top Ten 2014. This covers insecure data storage and unintended data leakage.

## **M3 - Insecure Communication**

This covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc.

## **M4 - Insecure Authentication**

This category captures notions of authenticating the end user or bad session management. This can include:

- Failing to identify the user at all when that should be required
- Failure to maintain the user's identity when it is required
- Weaknesses in session management

## **M5 - Insufficient Cryptography**

The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, that probably belongs in M2. This category is for issues where cryptography was attempted, but it wasn't done correctly.

[https://www.owasp.org/index.php/Mobile\\_Top\\_10\\_2016-Top\\_10](https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10)

# Mobile application

- OWASP – Mobile top 10 critical mobile security flaws - 2016

## **M6 - Insecure Authorization**

This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, forced browsing, etc.). It is distinct from authentication issues (e.g., device enrolment, user identification, etc.).

If the app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then that is an authentication failure not an authorization failure.

## **M7 - Client Code Quality**

This was the "Security Decisions Via Untrusted Inputs", one of our lesser-used categories. This would be the catch-all for code-level implementation problems in the mobile client. That's distinct from server-side coding mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that's running on the mobile device.

## **M8 - Code Tampering**

This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification.

Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.

## **M9 - Reverse Engineering**

This category includes analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA Pro, Hopper, otool, and other binary inspection tools give the attacker insight into the inner workings of the application. This may be used to exploit other nascent vulnerabilities in the application, as well as revealing information about back end servers, cryptographic constants and ciphers, and intellectual property.

## **M10 - Extraneous Functionality**

Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example includes disabling of 2-factor authentication during testing.

[https://www.owasp.org/index.php/Mobile\\_Top\\_10\\_2016-Top\\_10](https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10)



# Mobile – physical risk

- Lost or stolen in public areas
- Data may be sensitive (list of calls, texts, calendar)
- Sensitive accounts linked with mobile devices
- Sensitive data “all in one place”

# Mobile – mitigate risk

- Cell-based tracking and locating device
- Remote shutdown with wipe capabilities
- Remote SIM card lock capabilities

# **Mobile – organizational risk**

- Pervasive in organization
- Corporate provisions or BYOD programs
- C-suite level and senior manager rely on mobiles
- Increase in complexity, settings, etc.

# Mobile – Technical risk

**Figure 6.6—Activity Monitoring and Data Retrieval Risk<sup>79</sup>**

Target	Risk
Messaging	Generic attacks on SMS text, MMS-enriched transmission of text and contents
	Retrieval of online and offline email contents
	Insertion of service commands by SMS cell broadcast texts
	Arbitrary code execution via SMS/MMS
	ML-enabled SMS text or email
	Redirect or phishing attacks by HTML-enabled SMS text or email
Audio	Covert call initiation, call recording
	Open microphone recording
Pictures/Video	Retrieval of still pictures and videos, for instance, by piggybacking the usual “share” functionality in most mobile apps
	Covert picture or video taking and sharing, including traceless wiping of such material
Geolocation	Monitoring and retrieval of GPS positioning data, including date and time stamps
Static data	Contact list, calendar, tasks, notes retrieval
History	Monitoring and retrieval of all history files in the device or on SIM card (calls, SMS, browsing, input, stored passwords, etc.)
Storage	Generic attacks on device storage (hard disk or solid state disk [SSD]) and data replicated there

# Mobile – Unauthorized network connectivity

**Figure 6.7—Unauthorized Connectivity Risk<sup>80</sup>**

Vector	Risk
Email	Simple to complex data transmission (including large files)
SMS	Simple data transmission, limited command and control (service command) facility
HTTP get/post	Generic attack vector for browser-based connectivity, command and control
TCP/UDP socket	Lower-level attack vector for simple to complex data transmission
DNS exfiltration	Lower-level attack vector for simple to complex data transmission, slow but difficult to detect
Bluetooth	Simple to complex data transmission, profile-based command and control facility, generic attack vector for close proximity
WLAN/WiMAX	Generic attack vector for full command and control of target, equivalent to wired network

**Command and control** functionality often found in malware requires a direct link between the mobile device and the attacker – vectors used shown above

# Mobile – Sensitive data leakage

**Figure 6.8—Sensitive Data Leakage Risk<sup>81</sup>**

Type of Information	Risk
Identity	International Mobile Equipment Identity (IMEI), manufacturer device ID, customized user information
	Hardware/firmware and software release stats, also disclosing known weaknesses or potential zero-day exploits
Credentials	User names and passwords, keystrokes
	Authorization tokens, certificates (S/MIME, PGP, etc.)
Location Files	GPS coordinates, movement tracking, location/behavioral inference
	All files stored at operating system/file system level

# **Mobile – Unsafe sensitive data storage / transmissions**

- Data stored often unencrypted
- Data is often stored in cloud services (personal, unmanaged)
- Sensitive data over WiMax, WLAN, near-field communication (NFC)
- Memorizing SSIDs increased evil twin threat
- No VPN on device

**Any questions?**



Section 6.4

**Consumerization of IT and mobile  
devices**

# Consumerization of IT and mobile devices

- Mobile devices is part of business
- Increased productivity and flexibility
- New business models have been developed as a result
  - Subscriptions
  - Payment tools
  - Pay-as-you-GO
- Opened the door to application development for devices
  - Note-taking
  - Video conferencing
  - Chatting
  - Cloud storage
  - Etc.

# BYOD pros / cons

Figure 6.9—Pros and Cons of BYOD

## Pros

- Shifts costs to user
- Worker satisfaction
- More frequent hardware upgrades
- Cutting-edge technology with the latest features and capabilities

## Cons

- IT loss of control
- Known or unknown security risk
- Acceptable Use Policy is more difficult to implement
- Unclear compliance and ownership of data

# Internet of things (IoT)

- **IoT:** Physical objects that have embedded network and computing elements that communicate with other objects over a network
- IoT is transforming business models and creating a new services

Business Risk	Operational Risk	Technical Risk
Health safety	Inappropriate access to functionality	Device vulnerabilities
Regulatory compliance	Shadow usage	Device updates
User privacy	Performance	Device management
Unexpected costs		

# Internet of things (IoT)

Figure 6.10—IoT Dos and Don'ts

## Dos

- Prepare a threat model.
- Evaluate business value.
- Holistically evaluate and manage risk.
- Balance risk and rewards.
- Notify all stakeholders of anticipated usage.
- Engage with business teams early.
- Gather all stakeholders to ensure engagement and thorough planning.
- Look for points of integration with existing security and operational protections.
- Examine and document information that is collected and transmitted by devices to analyze possible privacy impacts.
- Discuss with relevant stakeholders when, how and with whom that information will be shared and under what circumstances.

## Don'ts

- Deploy quickly without consulting business or other stakeholders.
- Disregard existing policy requirements, such as security and privacy.
- Ignore regulatory mandates.
- Assume vendors (hardware, software, middleware or any other) have thought through your particular usage or security requirements.
- Disregard device-specific attacks or vulnerabilities.
- Discount privacy considerations or “hide” data that are collected/transmitted from end users.

# Big data

- Data trend
- Big data represents a trend in technology that is leading the way to a new approach in understanding the world and making business decisions.
- Relies on very large unstructured, structured and complex data which makes it difficult to use ordinary tools

## **Possible risks to consider:**

- **Amplified technical impact**—If an unauthorized user were to gain access to centralized repositories, it puts the entirety of those data in jeopardy rather than a subset of the data.
- **Privacy (data collection)**—Analytics techniques can impact privacy; for example, individuals whose data are being analyzed may feel that revealed information about them is overly intrusive.
- **Privacy (re-identification)**—Likewise, when data are aggregated, semi-anonymous information or information that is not individually identifiable information might become non-anonymous or identifiable in the process

**Any questions?**

Section 6.5

**Cloud and digital collaboration**



# Cloud and digital collaboration

- Cloud computing offers a way to save on the capital expenditure associated with traditional methods of managing IT

Common platforms:

- Software as a service (SaaS)
- Platform as a service (PaaS)
- Infrastructure as a service (IaaS)
- Virtualization and Service-oriented architectures (SOAs)

# Risk of cloud computing

- **Loss of governance**—The client usually relinquishes some level of control to the cloud provider, which may affect security, especially if the service level agreements (SLAs) leave a gap in security defenses
- **Lock-in**—It can be difficult for a client to migrate from one provider to another, which creates a dependency on a particular cloud provider for service provision
- **Isolation failure**—One characteristic of cloud computing is shared resources. Although not commonplace, the failure of mechanisms that separate storage, memory, routing and reputation between different tenants can create risk
- **Compliance**—Migrating to the cloud may create a risk in the organization achieving certification if the cloud provider cannot provide compliance evidence.

# Risk of cloud computing

- **Management interface compromise**—The customer management interface can pose an increased risk because it is accessed through the Internet and mediates access to larger sets of resources
- **Data protection**—It may be difficult for clients to check the data handling procedures of the cloud provider.
- **Insecure or incomplete data deletion**—Because of the multiple tenancies and the reuse of hardware resources, there is a greater risk that data are not deleted completely, adequately or in a timely manner
- **Malicious insider**—Cloud architects have extremely high-risk roles. A malicious insider could cause a great degree of damage

# Benefits of cloud computing

- **Market drive**—Because security is a top priority for most cloud customers, cloud providers have a strong driver for increasing and improving their security practices
- **Scalability**—Cloud technology allows for the rapid reallocation of resources, such as those for filtering, traffic shaping, authentication and encryption, to defensive measures
- **Cost-effective**—All types of security measures are cheaper when implemented on a large scale. The concentration of resources provides for cheaper physical perimeter and physical access control and easier and cheaper application of many security-related processes
- **Timely and effective updates**—Updates can be rolled out rapidly across a homogeneous platform
- **Audit and evidence**—Cloud computing can provide forensic images of virtual machines, which results in less downtime for forensic investigations

# **Social media risk – Corporate use**

- Introduction of viruses/malware to the organizational network
- Misinformation or misleading information posted through a fraudulent or hijacked corporate presence
- Unclear or undefined content rights to information posted to social media sites
- Customer dissatisfaction due to an expected increase in customer service response quality/timeliness
- Mismanagement of electronic communications that may be impacted by retention regulations or ediscovery

# **Social media risk – Employee use**

- Use of personal accounts to communicate work-related information
- Employee posting of pictures or information that link them to the enterprise
- Excessive employee use of social media in the workplace
- Employee access to social media via enterprise-supplied mobile devices (smartphones, tablets)

**Any questions?**

**Thank You**