# Cyber Situational Awareness and Opportunities for Future Enhancement

Michael Kalkavouras

Accenture Technology Consulting

michael.kalkavouras@accenture.com

# Look Out …

If you can’t pull the pieces together to see the attack coming, all you can do is try to recover from the damage. In the same vein, organizations are looking to gain additional insight into themselves and the world around them.

## A lack of “something”

*Graphic From http://demotivationalblog.com/

# Agenda

The seriousness of today’s situation

Key principles of cyber security

Current and emerging trends for the years ahead

# Real-Life Incidents

- Large Scale IP Theft
- Cyber Crime
- Industrial Espionage
- Control System Disruption

**Global internet slows after 'biggest attack in history**
The internet around the world has been slowed down in what security experts are describing as the biggest cyber-attack of its kind in history.
***http://www.bbc.co.uk***

**Hackers follow business shift to cloud computing**
Security experts warn cloud computing in Australia is becoming an increasingly appealing target for hackers as businesses rapidly take up the technology….
*http://www.abc.net.au*

**Anonymous threatens cyber attack on Israel**
Members of the Anonymous hacktivist have threatened cyber strikes on Israel within days of issuing a similar threat against North Korea
*http://motherboard.vice.com*

**Targeted attacks the next step in mobile malware**
The Android threat landscape continues to evolve in 2013. To distribute Android threats, malware authors are transitioning away from attacking traditional vectors like the Google Play Market and third-party Android markets to vectors like spam and phishing emails and SMS….
*http://blogs.mcafee.com*

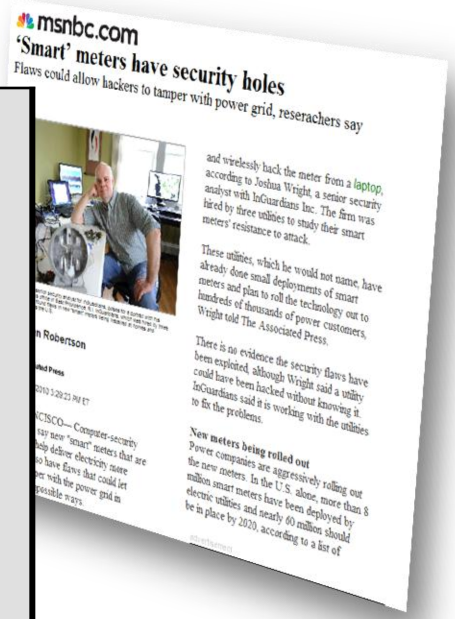
**NHS wor**

**The NHS has repo highest number of breaches of any UK organisation since 2007, the Informatio Commissioner's Offic**

David Smith, deputy co at the ICO told the Infos security conference the highlighted 287 breaches the period.

That accounts for more tha of the total number reported

**40 Million Vis**
**Express Rec**



msnbc.com

**'Smart' meters have security holes**

Flaws could allow hackers to tamper with power grid, reseracher say

n Robertson

ated Press

2010 3:29:23 PM ET

NCISCO— Computer-security say new "smart" meters that are help deliver electricity more so have flaws that could let per with the power grid in possible ways.

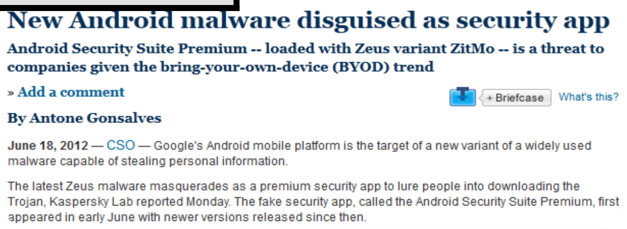
and wirelessly hack the meter from a laptop, according to Joshua Wright, a senior security analyst with InGuardians Inc. The firm was hired by three utilities to study their smart meters' resistance to attack.

These utilities, which he would not name, have already done small deployments of smart meters and plan to roll the technology out to hundreds of thousands of power customers, Wright told The Associated Press.

There is no evidence the security flaws have been exploited, although Wright said a utility could have been hacked without knowing it. InGuardians said it is working with the utilities to fix the problems.

**New meters being rolled out**
Power companies are aggressively rolling out the new meters. In the U.S. alone, more than 8 million smart meters have been deployed by electric utilities and nearly 60 million should be in place by 2020, according to a list of

advertisement



**New Android malware disguised as security app**

**Android Security Suite Premium -- loaded with Zeus variant ZitMo -- is a threat to companies given the bring-your-own-device (BYOD) trend**

» Add a comment

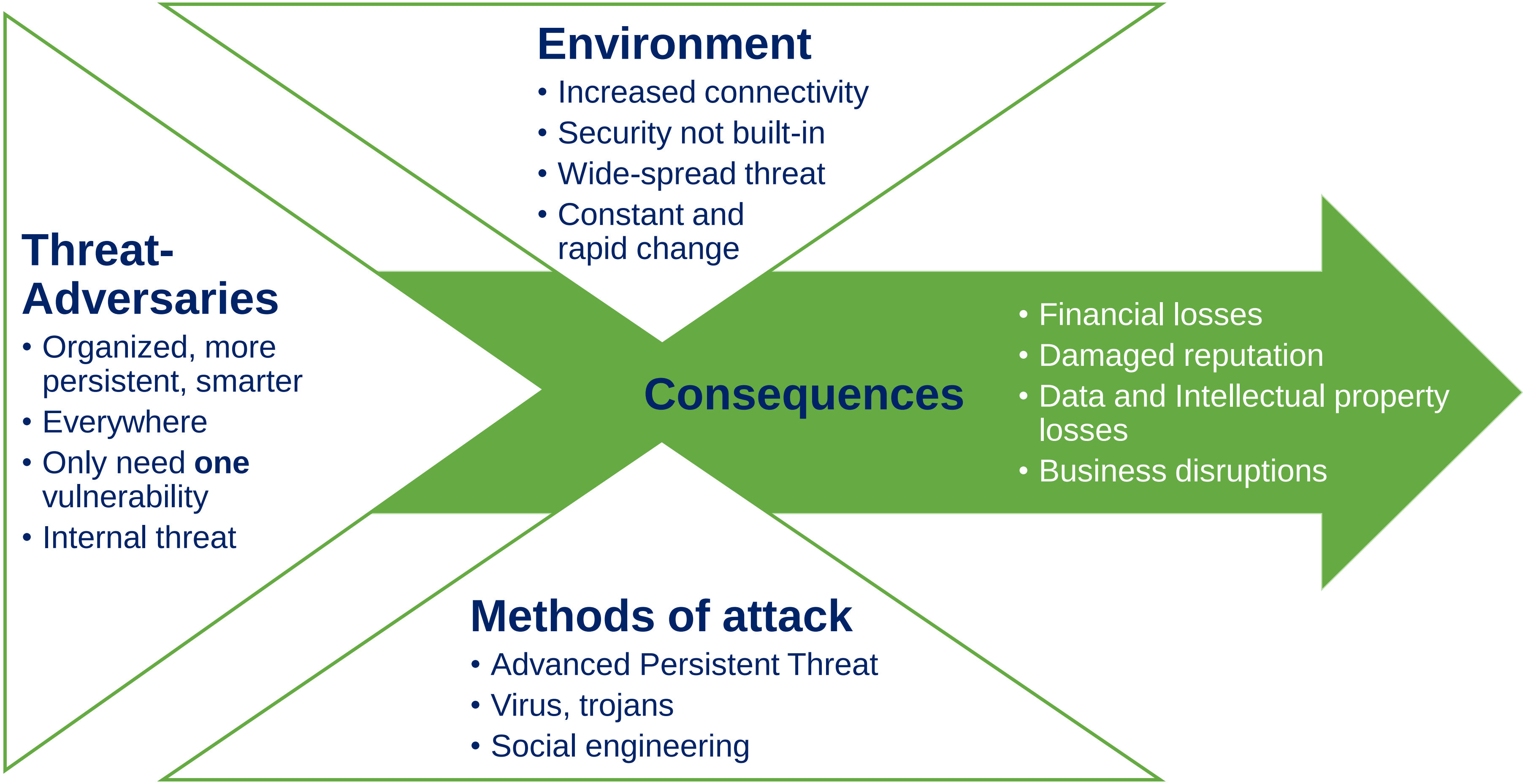
**By Antone Gonsalves**

**June 18, 2012** — CSO — Google's Android mobile platform is the target of a new variant of a widely used malware capable of stealing personal information.

The latest Zeus malware masquerades as a premium security app to lure people into downloading the Trojan, Kaspersky Lab reported Monday. The fake security app, called the Android Security Suite Premium, first appeared in early June with newer versions released since then.

# The cyber security ecosystem

**Understanding the adversary, the environment and the methods of attack is the only way to create a sound cyber security strategy today.**



## Threat-Adversaries

- Organized, more persistent, smarter
- Everywhere
- Only need **one** vulnerability
- Internal threat

## Environment

- Increased connectivity
- Security not built-in
- Wide-spread threat
- Constant and rapid change

## Consequences

- Financial losses
- Damaged reputation
- Data and Intellectual property losses
- Business disruptions

## Methods of attack

- Advanced Persistent Threat
- Virus, trojans
- Social engineering

**“Cyber threats directed against the United States are more diverse, interconnected and viral than at any time in American history”. James R. Clapper, the director of national intelligence**

# The environment

- **Corporations operate in the cyber space.** Every aspect of the business depends on Internet-oriented computing and communications.
- **Security is not built in.** Systems that designers assumed would operate behind physical or logical barriers are now accessible via networks.
- **Change is constant.** A “good enough” defense today won't be good enough in six months.
- **Corporations are lucrative targets.** Attackers can gain intellectual property, personally identifiable information, sensitive competitive data, etc.
- **No one is immune.** “On March 28 2013, American Express’ website went offline for at least two hours during a distributed denial of service attack……” “The newest wave of cyber-attacks targeting U.S. banks - which have cost millions of dollars since September - seem bent on destruction rather than espionage, Nicole Perlroth and David Sanger of The New York Times report….”

**And the list goes on.**

# The adversary

**Today's intruders rarely fit the image of a lone wolf probing corporate systems for bragging rights.**

- Adversaries are smarter, better organized, more persistent. Many are part of criminal organizations, some are agents for nation-states.
- Attackers have a huge advantage. In cyber, offense is far cheaper and easier than defense, which must be 100% effective. The adversary needs only to find one weakness.
- Variety of adversaries and motivations leads to variety of attack types.

# The methods of attack

## Adversaries only need to find one vulnerability— their methods of attack are multiple and rapidly changing

- Advanced Persistent Threats are targeted, “low and slow” attacks that stealthily move through a network without generating regular or predictable network traffic.
- U.S. military’s worst attack was launched from USB thumb drive bearing malicious program from foreign intelligence agency.
- Virus hidden on legitimate websites infected British bank customers’ computers, stole money from their online accounts.
- Google attack began with instant message sent to Google employee, who clicked a link to a poisoned website.
- Some attackers infect commercial software, hardware with “logic bombs” before it is sold.

# Threats from within

**Many of today’s cyber security threats result from the behavior of organizations’ employees.**

- Using popular social networking Websites, possibly exposing employers’ computers and networks to worms, malware, etc.
- Checking corporate email from unsecured personal devices, including smart phones and home computers.
- Self-provisioning potentially unsecure cloud-based applications.
- Accessing organization data from unsecure WIFI hotspots.

# Security breaches have serious business consequences

## Not just a technical issue

- In 2012, security breaches cost organizations an average of $2.4 million each—up from $2.2 million in 2011 and $2.1 million in 2010. *
- Stock prices of publicly-held companies typically drop five percent when breaches are made public.
- Fines and lawsuit losses can exceed $100 million.
- The loss of intellectual property due to cyber attacks can be significant.
- Cyber attacks can disrupt business operations (production interruptions, inability to process sales, etc.).
- Brand reputation and consumer and partner trust can be severely damaged by a data breach.

* Third Annual Benchmark Study on Patient Privacy & Data Security, December 2012, Ponemon Institute

# The key principles of cyber security

1. Identify and secure the IT assets themselves, not just the perimeter.
2. Build a hard-nosed “culture of security.”
3. Pay closer attention to applications.
4. Check and double-check user identity.
5. Develop acute situational awareness.

# 1. Identify and secure the IT assets themselves, not just the perimeter

- Identify data and technology that are essential to operations and business continuity (many large organization have not yet done so).
- Create a detailed plan to protect these assets and capabilities, not just the perimeter.
- Assure plan meets regulatory, compliance, privacy and business demands.
- Assure plan viability with robust test.
- Embed cyber resilience and defensive capabilities throughout the organization, not just individual components.

# 2. Build a hard-nosed “culture of security”

- Understand the **organizational risks** posture
- **Create measurable objectives** to support continuous improvement
- Obtain **support** for security initiatives **from the top of the pyramid**
- Use short, **high-impact messages** and real world examples at high frequencies to illustrate the true likelihood of security threats
- **Security awareness** is critical to maintaining a living security culture and using **dynamic** content presentation is vital to avoid diminishing impact.
- **Security is everyone’s responsibility** and must be part of every employee’s job description
- Define a **training plan** that is relevant to the specific workforces
- Create real **consequences for security violations** and enforce through strong policies
- Create a program to **reward positive security behaviors**
- Use **enabling technologies** to enforce security policies within the enterprise

# 3. Pay closer attention to applications

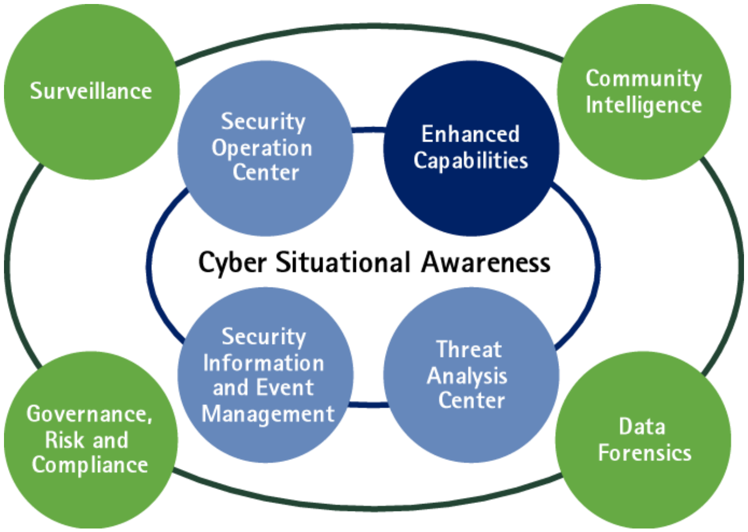
- Many serious breaches result from application-level weaknesses.
- Most developers have not included security in their applications, assuming the software would run inside a secure perimeter.
- Extend security to device level as well as to application layer.
- Measure security strength of off-the-shelf applications.

# 4. Check and double-check user identity

- Stop relying on authentication information (e.g. mother’s maiden name)  that has become more available or discoverable.
- Integrate strong authentication technologies with access management technologies.
- Biometrics (fingerprint, retinal scans), smart cards becoming more cost-effective.
- Embed pervasive security while maintaining ease of use (e.g. single sign-on, immediate access revocation, self-service functionality, real-time analysis).
- Consider two-factor authentication (e.g. smart card plus password).

# 5. Develop acute situational awareness

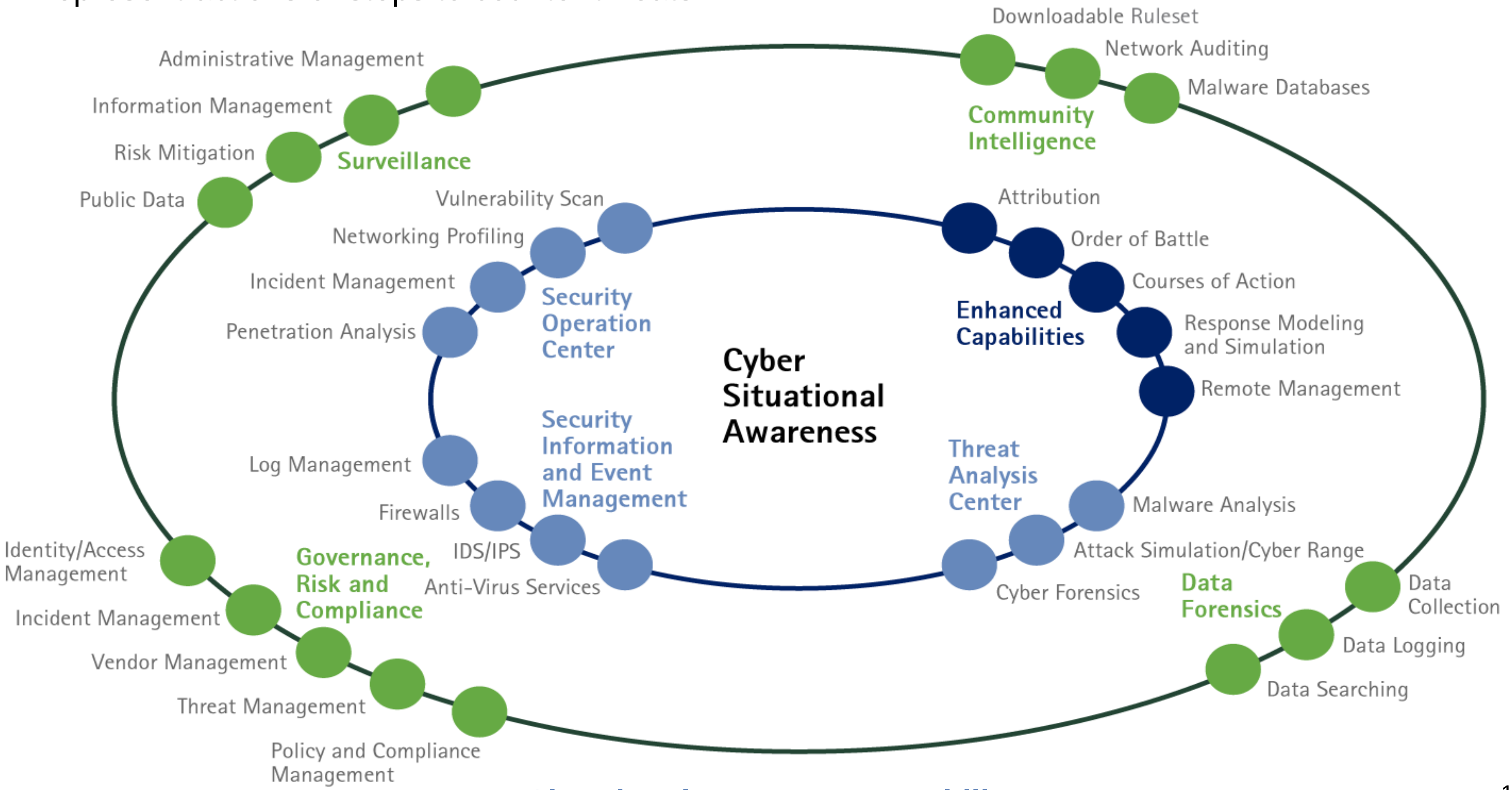
Situational awareness capability map


Surveillance
Security Operation Center
Enhanced Capabilities
Community Intelligence
Cyber Situational Awareness
Governance, Risk and Compliance
Security Information and Event Management
Threat Analysis Center
Data Forensics

- Attackers begin work long before detectable event.
- Organizations must:
  - Understand risk across entire landscape, including supply chain, business partners.
  - Recognize back doors and vulnerabilities.
  - Recognize complex and chained patterns that indicate attack initiation.
  - Expand scope of vulnerability assessment or penetration tests.
  - Harness external sources of threat intelligence.
  - Detect reconnaissance activity by a terminated employee or a hacker forum.

# Situational awareness capability map

Situation awareness capability mapping surfaces distinct cyber security capabilities that enable actions and those that enable intelligence. The outer circle in the diagram below represents sophisticated vendor & technology-driven data feeds and gathering activities, while the inner circles represent actions or steps to counter threats.



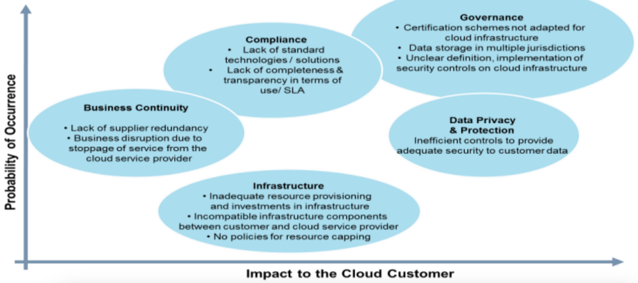
Situational awareness capability map

# Security Prediction: Current and Emerging Trends for the years ahead

According to the latest incidents, an increase of cyber attacks has been noticed in the following areas:

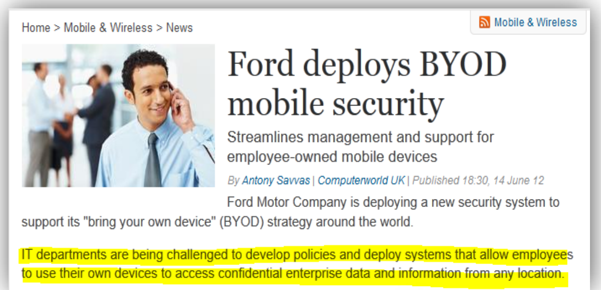
– Hackers follow business shift to **cloud computing**

Security experts warn cloud computing in Australia is becoming an increasingly appealing target for hackers as businesses rapidly take up the technology


Probability of Occurrence
Impact to the Cloud Customer
Governance
• Certification schemes not adapted for cloud infrastructure
• Data storage in multiple jurisdictions
• Unclear definition, implementation of security controls on cloud infrastructure
Compliance
• Lack of standard technologies / solutions
• Lack of completeness & transparency in terms of use/ SLA
Business Continuity
• Lack of supplier redundancy
• Business disruption due to stoppage of service from the cloud service provider
Data Privacy & Protection
Inefficient controls to provide adequate security to customer data
Infrastructure
• Inadequate resource provisioning and investments in infrastructure
• Incompatible infrastructure components between customer and cloud service provider
• No policies for resource capping

– Targeted attacks the next step in **mobile malware**

The Android threat landscape continues to evolve in 2013. To distribute Android threats, malware authors are transitioning away from attacking traditional vectors like the Google Play Market and third-party Android markets to vectors like spam and phishing emails and SMS….



Home > Mobile & Wireless > News

Mobile & Wireless

Ford deploys BYOD mobile security

Streamlines management and support for employee-owned mobile devices

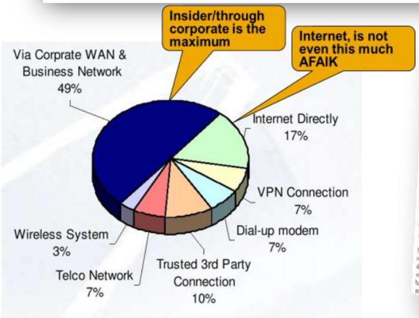
By Antony Savvas | Computerworld UK | Published 18:30, 14 June 12

Ford Motor Company is deploying a new security system to support its "bring your own device" (BYOD) strategy around the world.

IT departments are being challenged to develop policies and deploy systems that allow employees to use their own devices to access confidential enterprise data and information from any location.

– Cyber security coming to the forefront of **energy**'s attention

Globally, the Security Dept. found that internet-based attacks on critical U.S. energy infrastructure were occurring at a greater rate than previously thought, with 40% of those reported directed against the energy sector



Attack Vectors into ICS: 2003 - 2006 data from Eric Byres, BCIT

msnbc.com

'Smart' meters have security holes

Flaws could allow hackers to tamper with power grid, reserachers say

By Jordan Robertson

Associated Press

SAN FRANCISCO — Computer-security researchers say new "smart" meters that are designed to help deliver electricity more efficiently also have flaws that could let hackers tamper with the power grid in previously impossible ways.

and wirelessly hack the meter from a laptop, according to Joshua Wright, a senior security analyst with InGuardians Inc. The firm was hired by three utilities to study their smart meters' resistance to attack.

These utilities, which he would not name, have already done small deployments of smart meters and plan to roll the technology out to hundreds of thousands of power customers, Wright told The Associated Press.

There is no evidence the security flaws have been exploited, although Wright said a utility could have been hacked without knowing it. InGuardians said it is working with the utilities to fix the problems.

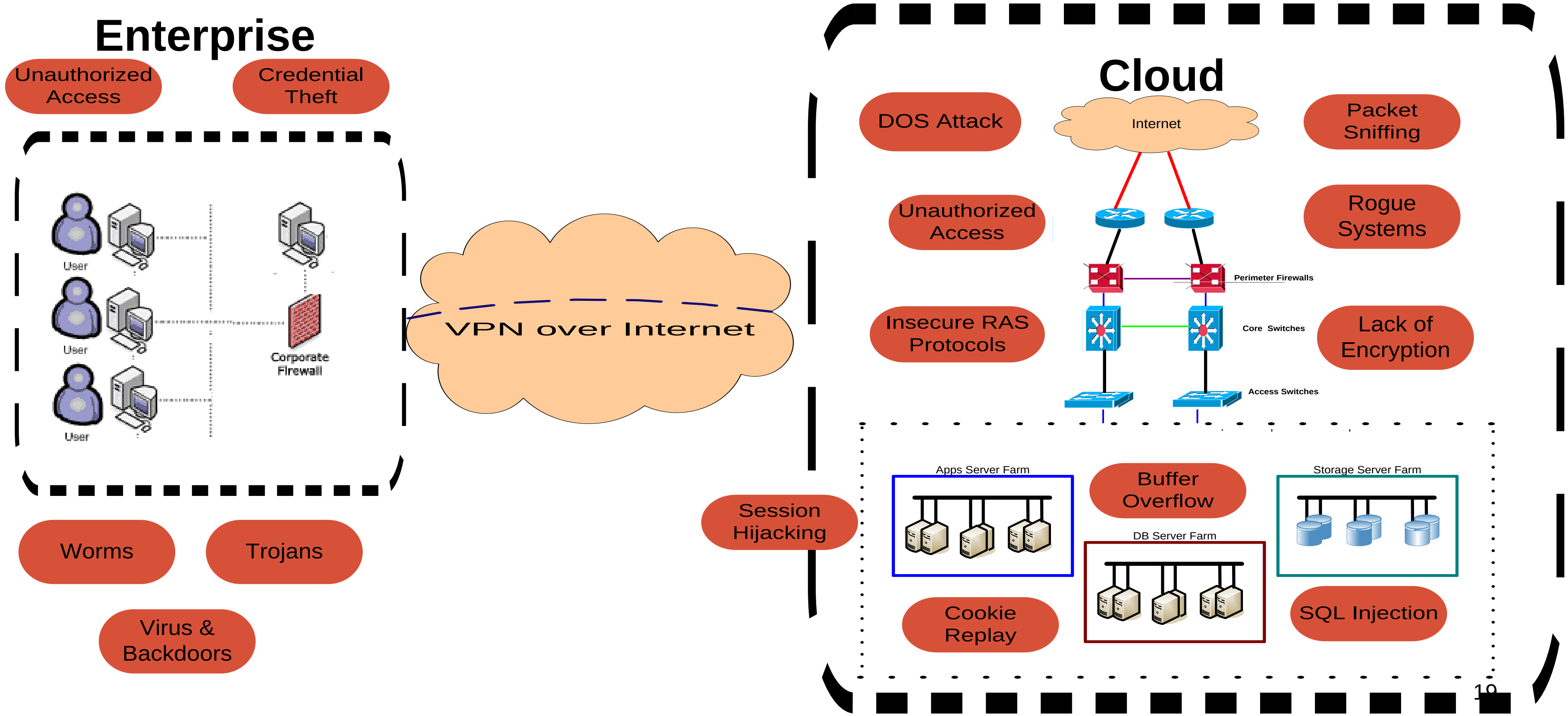
New meters being rolled out

Power companies are aggressively rolling out the new meters. In the U.S. alone, more than 8 million smart meters have been deployed by electric utilities and nearly 60 million should be in place by 2020, according to a list of

In the face of the current challenges, security needs to be **adaptable** and leverage an aligned approach **across the industries** around the globe

# Cloud Security Challenges – Technology

- Displayed below are sample threats and vulnerabilities, which can affect a Cloud Computing environment.
- Depending on the deployment model adopted, some of the threats might impact the enterprise, the provider or both.



Enterprise

Unauthorized Access

Credential Theft

Worms

Trojans

Virus & Backdoors

VPN over Internet

Cloud

DOS Attack

Packet Sniffing

Unauthorized Access

Rogue Systems

Insecure RAS Protocols

Lack of Encryption

Session Hijacking

Buffer Overflow

Cookie Replay

SQL Injection

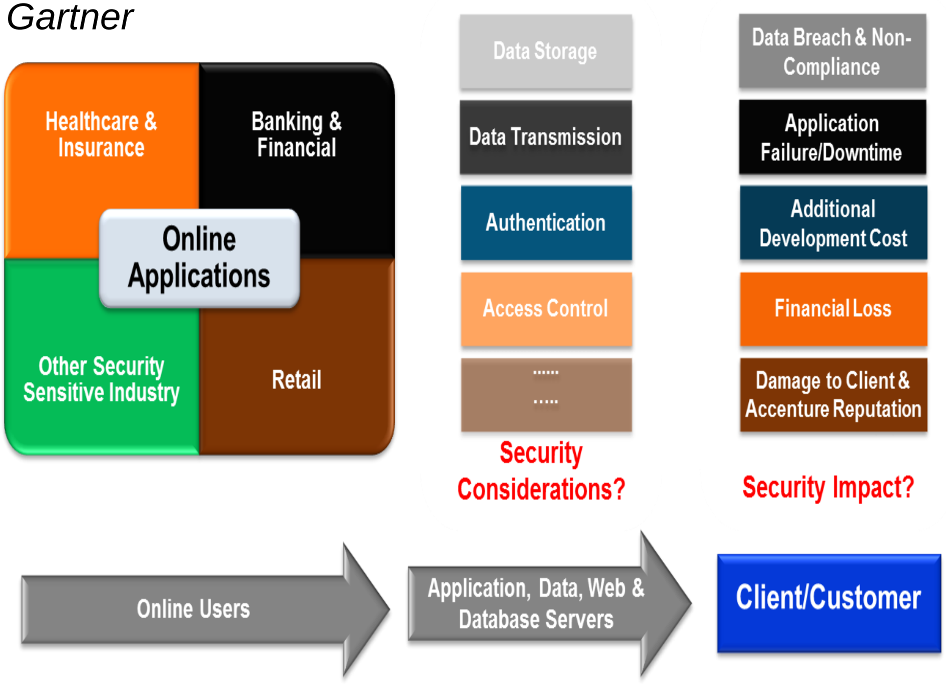
# Cloud Security Technology

| Risks/ Challenges | Solutions/ Recommendation |
|---|---|
| Challenges in user provisioning in IaaS for provisioning of both privileged and business users to VPN gateways, hosts, and applications. | Implementing strong authentication or a multi-factor authentication or authentication protected by cryptographic means. |
| Challenged in authentication in order to manage credentials including passwords, digital certificates, and dynamic credentials. | Authenticating users with the enterprise’s Identity Provider and establishing trust with the SaaS vendor by federation. |
| Denial of service attacks arising due to poor network security implementation. | Conducting internal and external penetration testing exercises to test the effectiveness of network security components. |
| Security issue such as long time readability of data archives, data archives, burden of proof and digital asset protection due to virtualization. | Perform shrinking of secured perimeter by leveraging on virtualization or workspace lightening. |
| Challenges arising due to data lifecycle management across cloud networks across various networks. | Implementing stringent controls around data lifecycle management for applications, infrastructure etc. |
| Challenges in data tampering during transmission over unsecured networks and storage areas. | Implementing effective encryption tools for securing data in order to avoid tampering and misuse. |

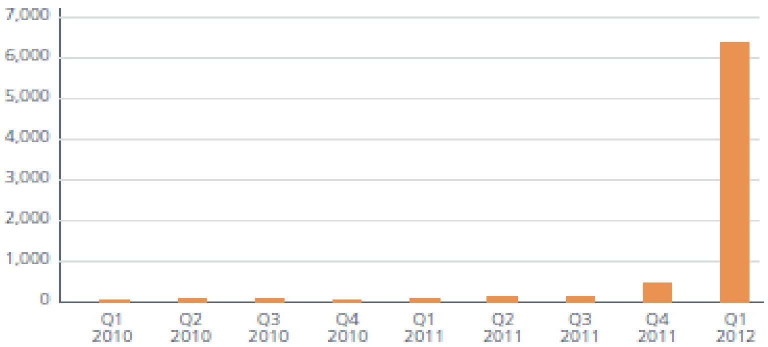
# Threats on Mobile Devices

## Increasing demand for content over the internet has increased the risk exposure of sensitive and confidential data

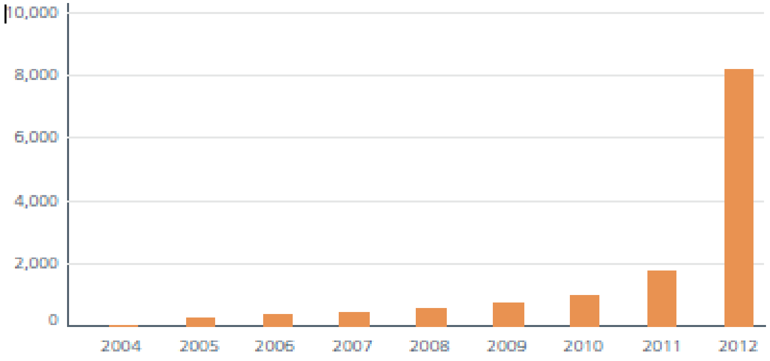
*“Enterprise boundaries continue to blur as data is shared across the Internet between partner organizations and unmanaged endpoints, increasing concerns about data leakage and manipulation. This is encouraging greater use of application layer and data layer security controls” -* Gartner



Source: McAfee Threats Report First Quater 2012



Total Mobile Malware Samples in the Database



New Mobile Malware

Source: Symantec Internet Security Threat Report, Volume 17-April 2012

# General Mobile Vulnerabilities and Risks

**Mobile applications**

- Feature-rich mobile applications can process and store sensitive information.
- Applications with integrated GPS feature can track a user’s location.

**Malicious code**

- Users are susceptible to malicious code (e.g. viruses, worms, trojans) that has been created specifically for the exploitation of mobile devices.

**Theft / loss of devices**

- Mobile devices, including laptop computers and smartphones, are relatively small and easy to steal or lose.

**Compromise via wireless technologies**

- WiFi, cellular (voice and data), and Bluetooth can be on one device
- Not only can data be stolen, but attackers can gain unauthorized access to private networks.

**Theft / loss of data**

- Compromised devices can be mined for sensitive data
- Attackers have become more sophisticated and can use forensic techniques to recover data that was thought to have been “deleted”

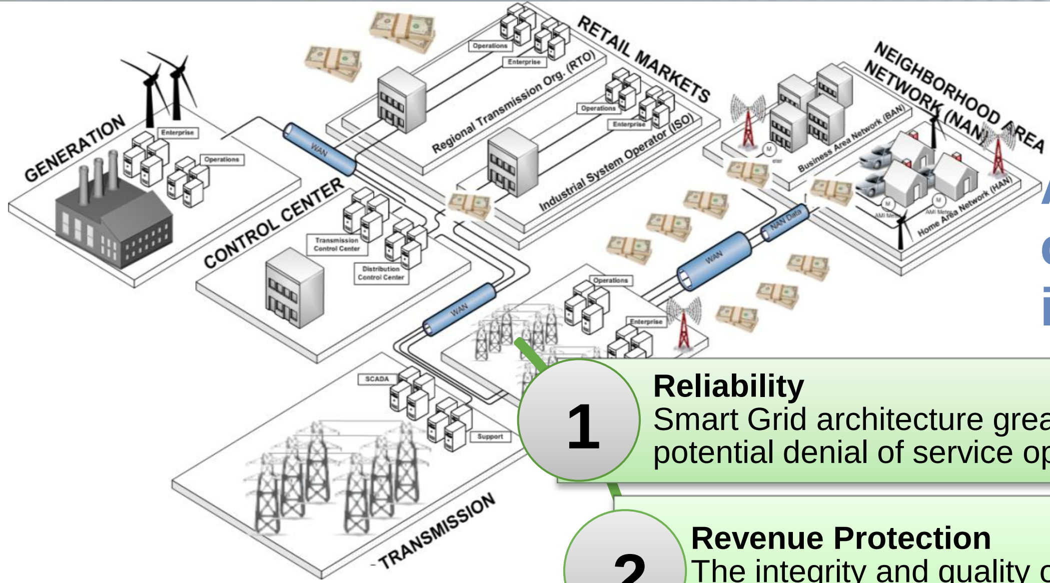
**Loss of productivity**

- Users expect to be able to work remotely, so if their devices or the networks are compromised resulting in a denial-of-service, productivity (and money) are lost.

**User awareness**

- Users of mobile technologies often lack the proper awareness and training of the risks posed by accessing corporate resources while mobile.

# Threats on Smart Grid



## Attackers will likely attempt to compromise the reliability, integrity, and privacy of the grid.

1. **Reliability**
   Smart Grid architecture greatly extends the network edge and introduces several potential denial of service opportunities to attackers
2. **Revenue Protection**
   The integrity and quality of field data must be maintained to support accurate billing for energy consumed
3. **Business Continuity/Disaster Recovery**
   Rapid recovery of Smart Grid systems will be essential for successful programs
4. **Privacy**
   Smart Grids enable collection of sensitive customer data that should be protected

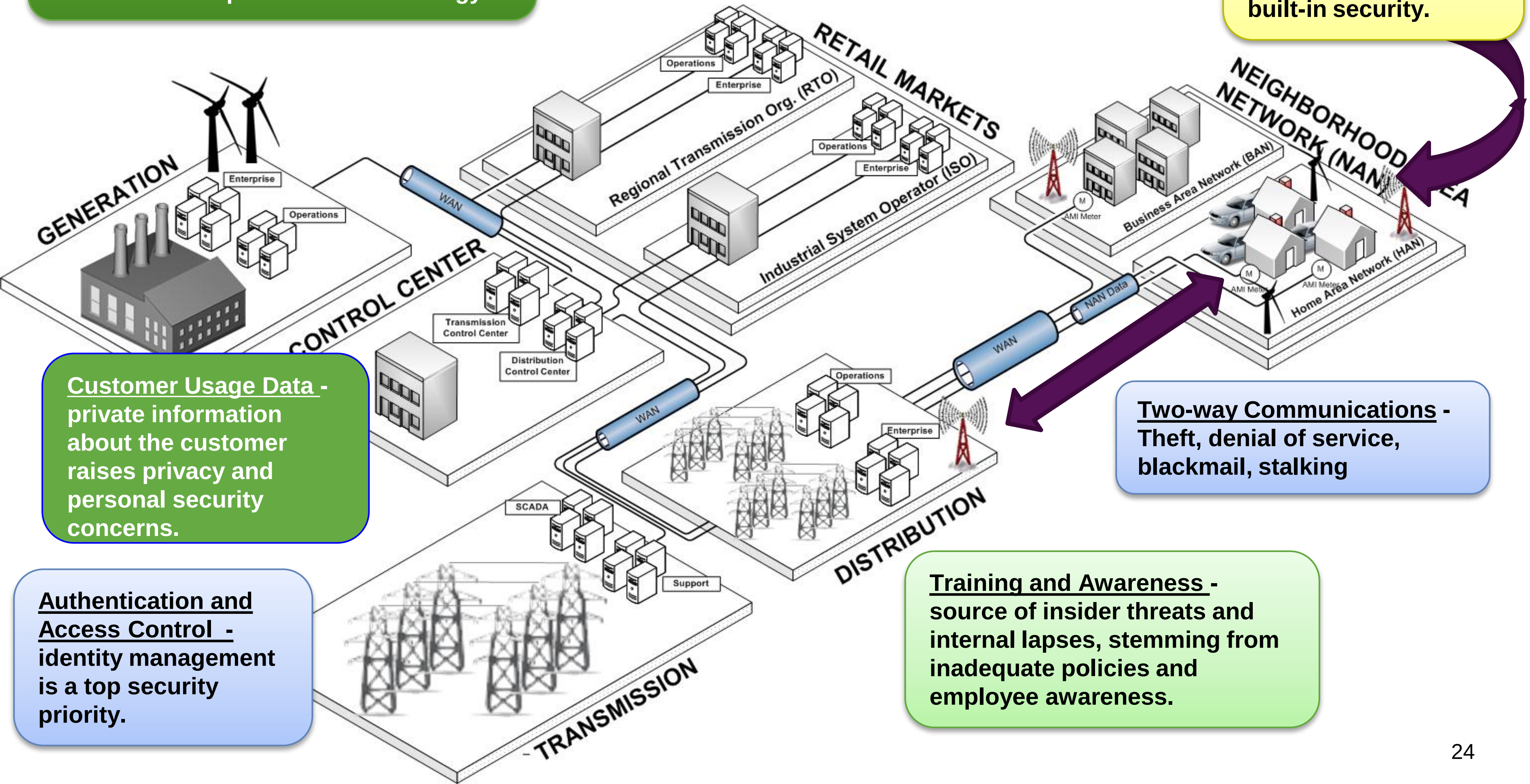
***Nationwide panic and chaos is less of a risk than obtaining free electricity***

# Smart Grid Vulnerabilities

**Lack of Standards and Interoperability** - smart grid equipment is a significant factor in how fast utilities and consumers adopt this new technology.

**Distributed Connectivity** - expanding boundary and increased exposure to threats. Millions of networked devices will be distributed across vast geographic regions.

**Metering Devices** - multiple manufacturers and varying levels of built-in security.



**Customer Usage Data** - private information about the customer raises privacy and personal security concerns.

**Two-way Communications** - Theft, denial of service, blackmail, stalking

**Authentication and Access Control** - identity management is a top security priority.

**Training and Awareness** - source of insider threats and internal lapses, stemming from inadequate policies and employee awareness.

# Asks / Questions / Discussion