Current threats, appropriate defences and the future lessons learned

Raj Kumar

Current threats, appropriate defences and the future lessons learned

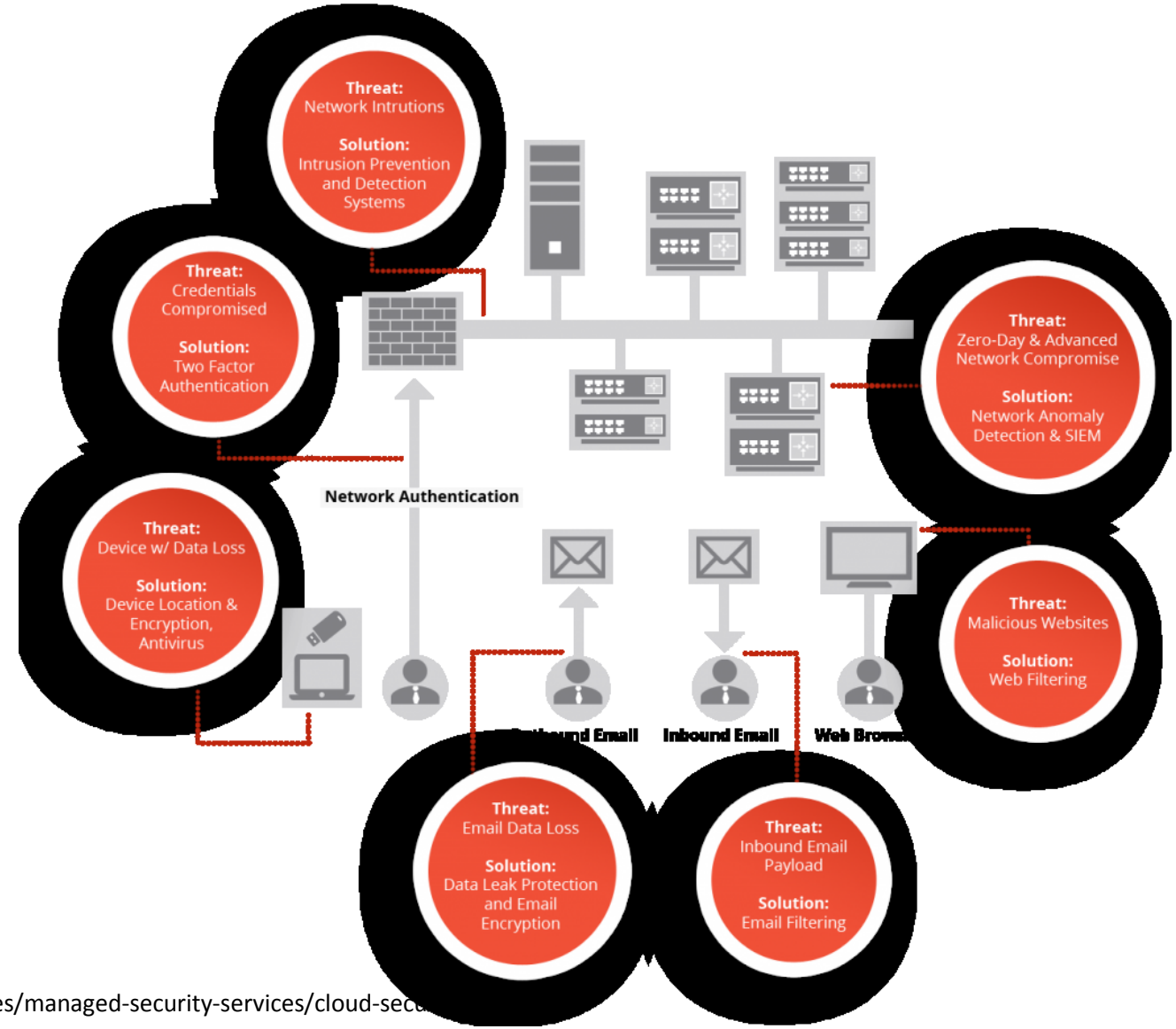
- Sharing analytics of data monitored and analysed
- Leveraging on NRIS Secure Technologies and Information Security Report

Top Corporate Cybersecurity Risks

Lack of cybersecurity measures	Not understanding cybersecurity risks	Lack of cybersecurity policy	Confusing compliance with cybersecurity	The human factor	Bring your own device and cloud
Funding and talent constraints	No information security training	Lack of recovery plan	Constantly evolving risk	Aging infrastructure	Corporate culture and inefficiencies
	Lack of accountability	Difficulty in integrating data sources	Reactive mindset	Disconnect between spending and implementation	

https://heimdalsecurity.com/blog/10-critical-corporate-cyber-security-risks-a-data-driven-list/

Are you managing all these IT threats?



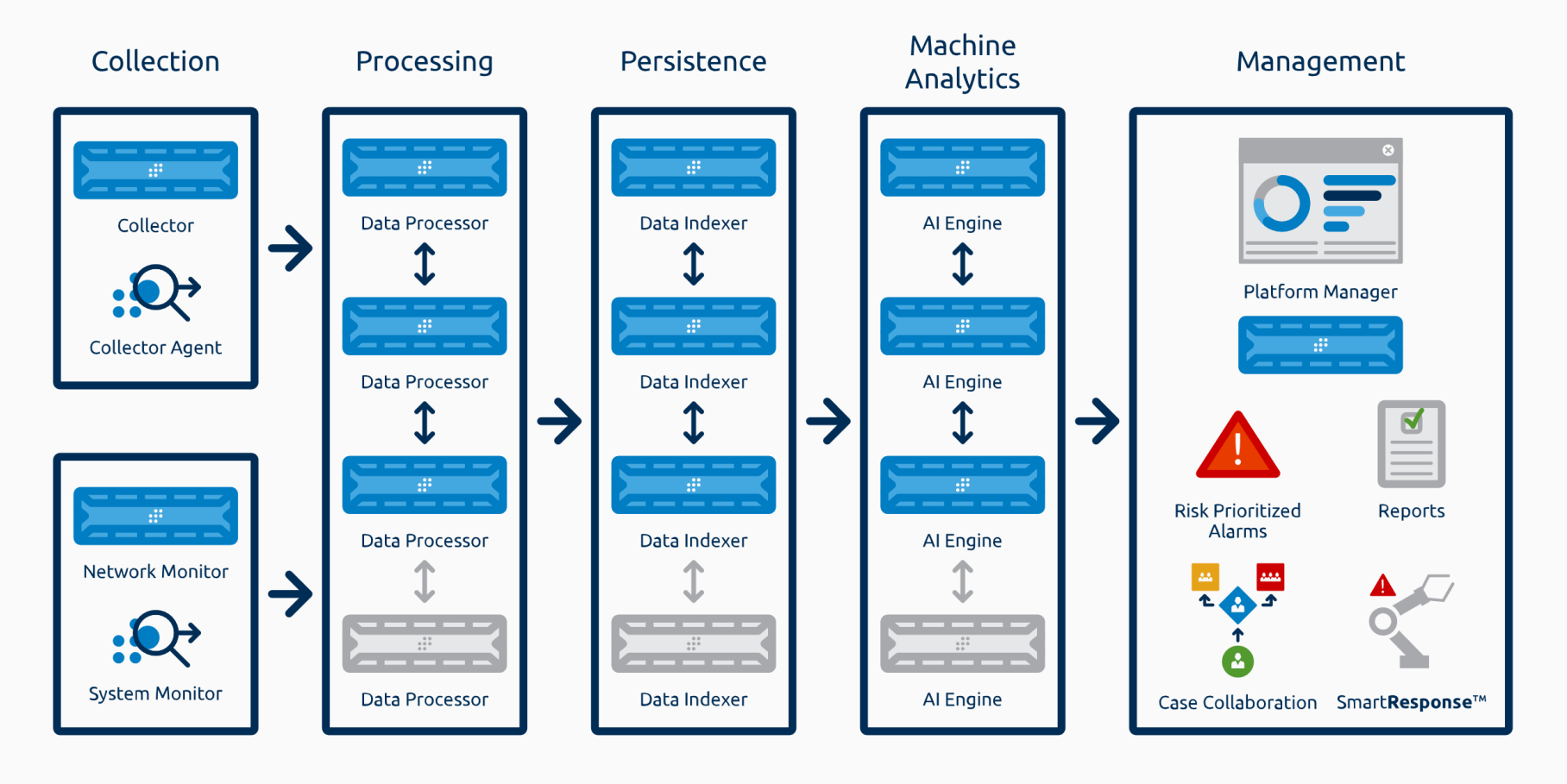
https://synoptek.com/it-infrastructure-services/managed-security-services/cloud-sec

CELEBRATING 25 YEARS OF ACHIEVEMENTS

Threat Analytics Platform

https://www.fireeye.com/products/threat-analytics-platform/threat-analytics-datasheet-pf-tap.html

Threat Analytics Platform



http://www.siemworks.com/SecurityIntelligence.asp

Use of AI in Threat Intelligence

- Automated, continuous analysis and monitoring of all activities in the environment
- Applies Threat intelligence – known and unknown
- Improved search over networks, many devices and applications
- Provides real-time visibility to risk, threat and operational issues
- Detect threats that are not detectable in practical way
- Scalable to meet business needs
- AI Engines are able to predict, detect and quicky respond to:
  - Intrusions
  - Insider Threats
  - Fraud
  - Behaviour anomalies with users, networks and endpoints
  - Compliance violation
  - Disruption to IT Services
  - Other actionable items

NRI Secure Technologies - NeoSOC

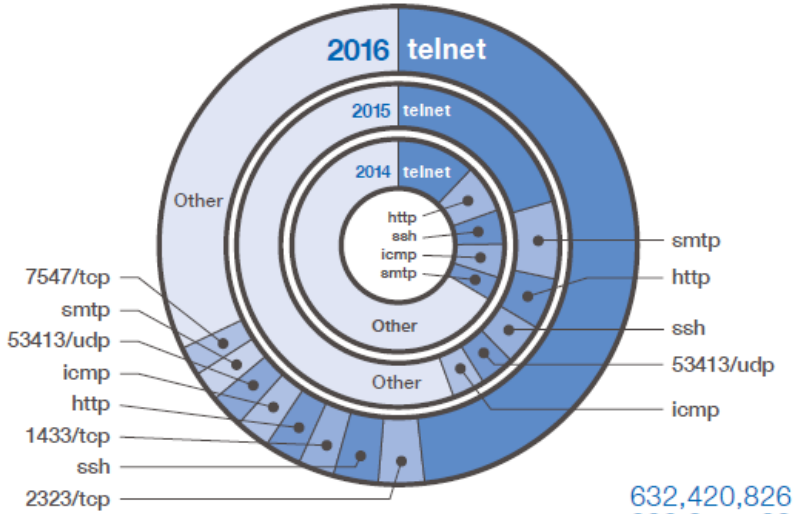
- Advanced detection tools and techniques using machine learning technology
- Provides security monitoring and alerting service with low-false positive rate
- Supports 400+ devices and applications as log sources to provide clear visibility into any security threats facing your organization
- Rapid deployment
- Actionable Alerts
- 24/7 security monitoring and alerting
- Save on training and focus on high value contextual security work
- Performs APT through custom use case threat modelling

NRI Secure - Information Security Report 2017

- Surge in access attempts targeting specific devices
- Recorded as the largest DDoS attack in history
- Mirai IoT Malware and its variants
- Restricting unauthorised external access to IoT devices not implemented
- IoT Devices need to assessed for security
- Devices must be securely configured and preventative measures must be taken
- IoT manufacturer must implement strict security controls in their devices

Significant Increase in Communications Targeting Weakly Managed IoT Devices

■ **Communication attempts blocked by firewall (by percentage)**

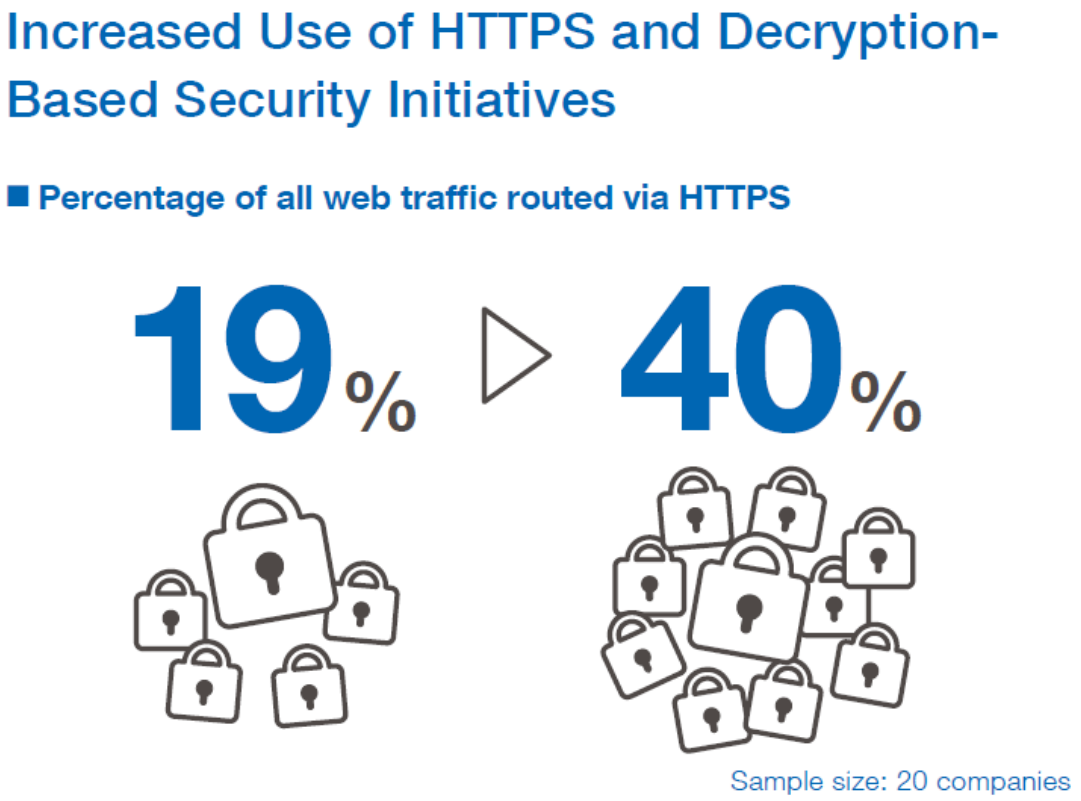


Sample size
632,420,826 attempts (2014)
808,955,599 attempts (2015)
2,262,695,083 attempts (2016)

CELEBRATING 25 YEARS OF ACHIEVEMENTS

NRI Secure - Information Security Report 2017

- HTTPs implementation has increased over the years
- Used by website handling highly confidential data
- Able to verify web server authenticity and prevents eavesdropping
- Antivirus programs don’t work well on communications routed through proxy servers
- Companies need to adapt security strategies to support enhanced security features on client devices
- Implement HTTPs decryption on communication route

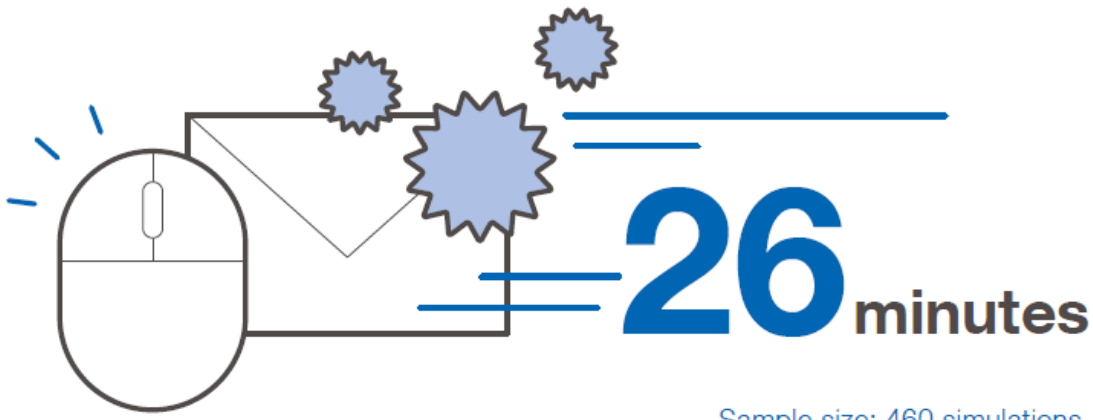


NRI Secure - Information Security Report 2017

- In 2017, increase in targeted mass distributed malware emails
- Employee need to be trained on how to recognise and avoid malware emails
- 26 minutes is ideal response window between detecting an attack and responding to the attack
- Employee need to understand the workflow for reporting attack emails

The 26 Minute Window until an Attack Email is Opened

■ Average time from when a training email was sent until a user opened an attachment or clicked a URL link in the email



Sample size: 460 simulations

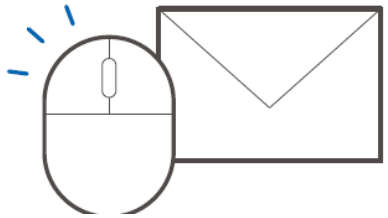
CELEBRATING 25 YEARS OF ACHIEVEMENTS

NRI Secure - Information Security Report 2017

- Targeted attack emails for the purpose of user education showed improvements
- Email training enhances understanding and exposes employee to actual attack methods
- Simulated email attack aims to educate employees on avoiding opening suspicious email and clicking on links

■ **Attachment/URL access rates in email training**

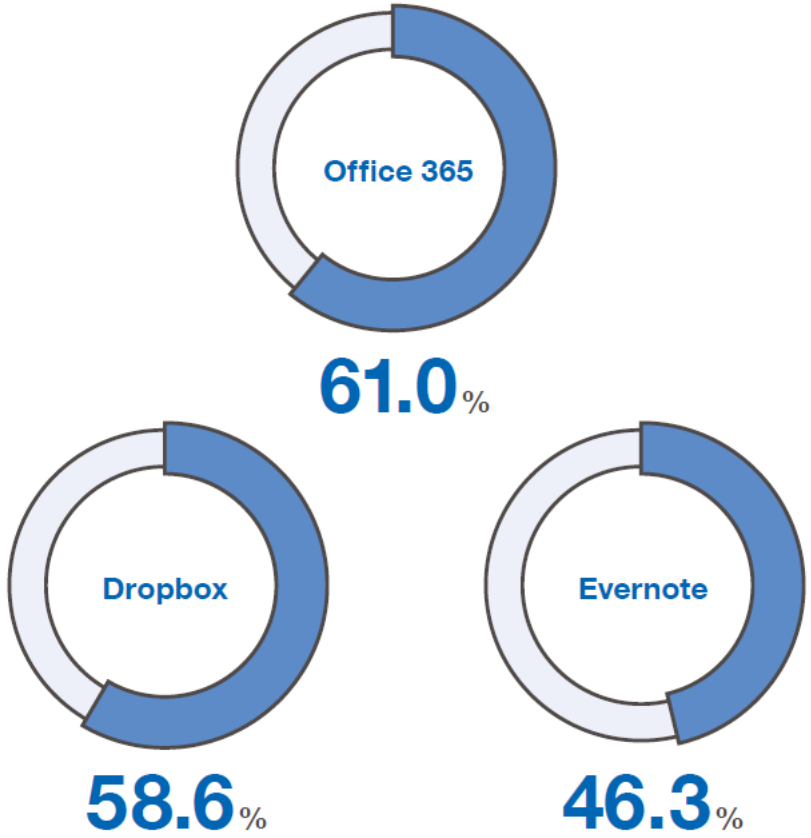
Survey period	Access rate
2012 (Apr.2012–Mar.2013) Sample size: 164,974 participants	22.5%
2013 (Apr. 2013–Mar.2014) Sample size: 101,326 participants	15.6%
2014 (Apr. 2014–Mar.2015) Sample size: 190,730 participants	15.3%
2015 (Apr. 2015–Mar.2016) Sample size: 565,115 participants	12.8%
2016 (Apr. 2016–Mar.2017) Sample size: 837,703 participants	**9.2** %



CELEBRATING 25 YEARS OF ACHIEVEMENTS

NRI Secure - Information Security Report 2017

- Cloud services poses threat for users and organisations
- NRI Secure found that 40.4% of the companies were using SaaS.
- Recent results show that some of the services were used individually without company approval
- Individual and departments using cloud services without approval which could be vector for information leak
- Unintended, errors in privacy setting and misconfiguration could lead to information leak



Sample size: 41 companies

CELEBRATING 25 YEARS OF ACHIEVEMENTS

Group Exercises

15 minutes for each scenario

Group Exercise 1

SCENARIO:

One of your organization's internal departments frequently uses public cloud storage to store large amounts of confidential and sometimes sensitive data. You have recently found out that the cloud storage provider has been publicly compromised and large amounts of data have been breached and exposed.

QUESTIONS:

1. What steps will your organization take?
2. Does your organization have policies that take into account storing information on public cloud storage?
3. Should your organization be held accountable for the data breach?
4. What actions and procedures would be different if this was a data breach on your own local area network?
5. What should management do? Who else in the organization should be involved?
6. What, if anything, do you tell your constituents? How and when would you notify them?

Group Exercise 2

SCENARIO:

You receive news that one of your employees has accidently disclosed sensitive personally identifiable information (PII) records for over 500 clients and personnel. This occurred when they accidentally emailed a document to a contractor. The employee had been recently trained on the handling of PII by your security team

QUESTIONS:

1. How does your organization handle this disclosure of PII?
2. Who do you contact regarding the disclosure?
3. Who would be responsible for taking the lead?
4. What policies or practices do you have in place to address the data loss?
5. What should management do? Who else in the organization should be involved?
6. Do you reprimand the employee?
7. What, if anything, do you tell your constituents who were NOT impacted?

Group Exercise 3

SCENARIO:

An employee casually remarks about how generous it is of government officials to provide the handful of USB drives on the conference room table, embossed with the government agency logo. After making some inquiries you find there were no instructions to provide USB drives to employees. Further investigation subsequently found an unspecified password-stealing keylogger on the USB drives. The spyware was designed to upload usernames and passwords to a server under the control of hackers.

QUESTIONS:

1. Who would the help desk notify?
2. How would you confirm the claim?
3. Who would you call to address the scenario?

Group Exercise 4

SCENARIO:

The browser deployed on all workstations in your organization has been infected with zero day vulnerability. You have already identified 10 workstations that are compromised as a result of this exploit and the help desk call volume due to this problem continues to increase abnormally. There is currently no vendor patch or vendor workaround. A patch is anticipated to be issued in one week.

Items to discuss:

1. What steps will you take to address the problem?
2. Who do you need to notify?
3. How will you determine if any sensitive data has been lost?
4. What impact will the exploit have on your agency and its operations?
5. Who is in charge?
6. What actions will you take post-event?

Group Exercise 5

SCENARIO:

Your organization's social media website is compromised.

Through public news outlets, an international terrorist group calling themselves the "Rebellion Cyber Forces" has displayed outrage against American politics. They have publicly claimed the successful cyber attacks on various government organizations. You learn that your organization's official social media accounts have been compromised and someone is sending out notifications through your social media website to your public claiming that your organization has been compromised by the rebellion cyber forces.

Items to discuss:

1. How would you be alerted if account takeover notifications were being sent from your social media account?
2. What steps will your organization take?
3. Who would be responsible for taking the lead?
4. What policies or practices do you have in place to address the situation?
5. What should staff do?
6. What should management do?
7. What, if anything, do you tell your constituents?
8. How or when would you notify them?

ITU : I Thank U