Cyber Security Trends

Vishakha Om Gupta
M.Tech. Department of Computer Science and Engineering
SIST, RGPV University Bhopal,
India

Arun R. Gupta
MCA, Computer Application Department
GGITS, RGPV University Jabalpur, India

***Abstract* — advanced cyber attacks and data theft schemes continue to evolve in both complexity and frequency. Whether state-sponsored, activist driven or criminally motivated, cyber-criminal activity continues to grow on a massive scale. A growing global criminal infrastructure is evolving in sophistication. Today, there seems to be an endless array of advanced attack methodologies and exploit kits easily purchased over the Internet. Unfortunately we are in an arms race. The level of sophistication around cyber crime continues to evolve and advance as companies struggle to adopt policies to prevent and respond to them. In most cases, companies are losing the war. In the case of Target, criminals stole credentials from a third-party vendor in order to embed malware on Target's point of sale registers. The sophistication and level of effort required to execute this breach highlights how every point in a company's logistics network can act as an entry point through which cyber criminals can enter. In 2014, the fear of a cyber attack and data security rank as one of the top five risks. In propose paper we are highlighting current cyber security trends and measure to reduce risk of that.**

Keywords— NIST, SLA, BYOD.

I. INTRODUCTION

Some of the information security trends we expect to see in upcoming years.

Cloud Insecurities - The growth of cloud computing continues to increase. More and more sensitive information is migrating to the cloud which puts that information at risk. Beyond a successful hacking event, imagine ransomware taking hostage of cloud hosted data [8]. The bad guys will continue to target endpoints, mobile devices and credentials in an effort to gain access to corporate and personal clouds.

Mobile Data on the Run – now days, there is significant increase in Android and Windows mobile malware across the globe. Criminals will continue to probe for weaknesses in the world's most popular mobile operating platforms. Mobile devices are an attractive launching pad for attacks aimed at social networks and cloud platforms. As corporations continue to embrace “Bring Your Own Device” (BYOD) policies in the work environment, cyber criminals will continue to explore opportunities to compromise devices and use them to access corporate networks.

Advance Persistent Threats, Persistently - An advanced persistent threat (APT) is an attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. Security experts are already seeing the blurring of the line between APT and traditional malware. New attacks will include strategies and delivery mechanisms specifically built to attack a more narrow targeted audience.

Social Re-engineering, Anti-social - Personal and business mobile apps will be fertile "watering holes" particularly for socially engineered scams and data exfiltration attempts. Address books and social connections are a treasure trove for bad guys. This information can be used to increase the sophistication and breadth of the cyber-crime.

Windows XP, a Window on your Soul - With Microsoft discontinuing support of the XP operating system, attacks on legacy systems will become commonplace. Without security updates, information on systems running XP will be increasingly at risk.

Hardware and Infrastructure Compromise - Incidents involving infrastructure and real world hardware are not only possible but have come to fruition. To date, very little focus and resources have been deployed to deal with this threat. Most companies will not have the resources or skill sets to identify these vulnerabilities. As more and more devices get connected to the "Internet of things," the security ecosystem becomes more complex and difficult to defend.

Increased Litigation - As more people and businesses are affected by information security breaches, the victims will attempt to hold the companies storing their sensitive information accountable. Customers whose identity has been stolen, shareholders affected by the decline in stock value of a company who has experienced a data breach and countless other breach scenarios will occur. Courts will need to grapple with defining reasonable conduct and liability thresholds.

Cyber Security Standards and Insurance - Standards will continue to evolve to create a framework that identifies reasonable Cybersecurity compliance. National Institute of Standards and Technology's (NIST) will continue to make progress in helping define "standards of care" [12]. The increased popularity in cyber insurance coverage will further drive the adoption of standards. Insurance companies, underwriting risk, will demand reasonable standards of care in both proactively defending against attack and reactively dealing with incidents after they have occurred [4].

Today, information security is not simply the responsibility of the IT department. The cyber security challenges facing companies are daunting, complex and dynamic. Companies must make cyber security one of their top priorities. All levels of the organization must come together to develop a holistic and comprehensive strategy that bridges the gap between technology, risk management, and cyber security. In this paper, we are providing practical guidance on how organizations can prepare for these challenges and mitigate the potential risk.

A. *Cyber Crime Statistics*

- Cyber attacks increased 14 percent in 2013
- The average cost of a data breach in 2013 was $6,200,000.
- 85% of malicious links used in web or email attacks were located on compromised legitimate websites.
- 3.3% of all spam contained malicious links and other malicious content.
- Nearly 145,000 new malicious programs for mobile devices were detected in 2013, more than tripling the previous year’s figure.

II. TOP SECURITY TRENDS AND HOW TO REDUCE RISK OF THAT

Cyber threat attacks and data theft themes continue to evolve in both complexity and frequency. In this paper we provide insight into reducing your company’s risk in these top security trends:

- Cloud computing
- Mobile computing
- Advanced persistent threat
- Social engineering.

A. *Cloud Computing*

The adoption of cloud computing is accelerating at an exponential pace. The level of security varies widely from one cloud provider to another, making it all the more critical for companies to manage the migration of information to the cloud very carefully. Public cloud computing introduces a third party into your data management strategy. This may create a higher level of risk when it comes to maintaining data integrity, adhering to privacy obligations and responding to a potential data incident [6].
Here are some important points to consider prior to migrate your data to the cloud:

- Assess the provider’s physical and digital security when considering a cloud solution.
- Evaluate your data before moving it to the cloud. Removing outdated information reduces risk. Identifying and properly classifying sensitive information allows you to consider additional security strategies for protecting against misuse and possible unauthorized access.
- Select cloud providers that have the necessary resources and expertise to scale and provide best in class security. Not all cloud provider options are created equal.
- Understand that you cannot outsource liability. Ultimately companies that move to the cloud still retain their legal liability as it relates to security and privacy.
- Consider the service level agreement (“SLA”) carefully [14].

Global rules on data privacy continue to evolve and no unifying standard exists. Users do not own the platforms where their data is being stored and cannot always ensure that the information is completely confidential and protected [8].
There is no way to completely be sure the information you store on the cloud is safe. However, the same is true for your corporate network. As said “you can take smart, preventative measures to better protect yourself.” With all this legal and technical uncertainty you have no choice but to take control and be responsible for your own data. All is not lost. Deploying some practical strategies can significantly reduce your exposure. Reduce or eliminate the storage of sensitive information in the cloud, read and negotiate service level agreement carefully, be serious about password management and encrypt your data.

B. *Mobile Computing*

Dual use devices have blurred the line between corporate and personal use. The risks associated with these mobile devices connected to corporate networks are abundant. Mobile devices are an attractive launching pad for attacks aimed at social networks and cloud platforms [9]. The security of mobile devices, often referred to as endpoints, are further complicated by the “Bring Your Own Device” (BYOD) trend. The number of devices and applications that need to be considered in a mobile security framework is daunting. IT professionals need to be concerned about the integrity of the physical devices and the applications running on them. Security professionals would be wise to consider how to protect both data at rest and data in transit. Data at rest refers to data stored on a device. Data in transit refers to how information flows over a network. A sound mobile data at rest security program considers ways to protect data from being hacked, stolen or lost, or inappropriately used by your employees. When considering data in transit, IT professionals should evaluate the security of wireless and VPN networks [7].
Even when corporate IT does not have a lot of oversight, there are some general best practices for securing data, including:

- Classify users. Employees may require different classifications. Different groups require different tools and access to different systems. Clearly define which mobile devise and back end systems each class of employee can access to help minimize the chaos.
- Acceptable mobile device list. Consider evaluating a core group of mobile devices that are deemed “safe.” Limiting access to a controlled number of devices helps facilitate effective information governance.
- Deployment and usage mapping. Develop a plan for deployment of acceptable devices. Maintain a detailed and dynamic list of devices that each employee uses. Standard operating procedures should be in place when deploying an acceptable device. By creating and keeping up-to-date a list of devices, a company will be

in a better position to deploy its strategies when an employee leaves the company or when a data loss event or other security scenario occurs.

- Governance and policy. This is an important area where organizations can quickly and efficiently improve their information security posture. IT controls, employee policies and training are fertile ground for cost effective and timely information security improvements.
- Risk assessment. Consider performing a security risk assessment to identify gaps. Once those gaps have been identified, rank them according to their importance and the company's acceptable risk parameters.
- Encryption. Companies must require encryption and remote wipe capabilities. Encrypting the data is one of the best ways to keep sensitive information safe. Good mobile data encryption techniques, including encryption for both on-device and transmitted data, can help in securing data and preventing corporate data from being compromised.
- Mobile device management software. To protect enterprise assets and personal devices, consider implementing a mobile device management program. Enterprise mobility management platforms provide a centralized manner of enforcing access control and authentication to apps and content on both corporate and user-owned devices.
- Mobile malware protection. Install smartphone malware protection on devices and educate users about securing data and responsible device-use practices.
- Back up. Regularly back up data on the mobile device.
- Delete sensitive information. Regularly delete any text messages or emails that contain sensitive information.
- Update and patch management. Ensure devices have the most up-to-date operating system and security patches.

The goal of mobile security should be to serve the needs of the business by establishing the best mobile user experience possible for the employee. Ideally, mobile security should be invisible to the end-user while still protecting corporate data. While that is not always possible, IT should find a balance between the users' experience and best practice security protocols.

C. *Advanced Persistent Threat*

Advanced persistent threat (APT) occurs when an unauthorized person gains access to a network and stays there undetected for a long time. There's a fine line between APT and malware [15]. APT is an attack on a specific target designed to gain access to a network and stealthily monitor the targeted computer systems for long periods of time. Some important and practical steps to protect from an APT attack:

- Identify and update a list of systems and assets that may be at risk.
- Develop an incident response plan prior to a crisis. Studies have shown that organizations with a well defined incident response plan reduce the time and damage associated with a data breach investigation. An important element of an incident response plan is to include rapid response tactics as time is of the essence [4].
- Deploy continuous monitoring tools designed to detect and identify viruses, malware, zero day exploits and APTs. Utilize intelligence based analysis of malicious domains and infrastructure, traffic anomalies and end-user behavior to identify infected devices.
- Maintain controls to prevent unauthorized escalation of user privileges and access to network resources. Restrict users to those network resources that are necessary to perform their jobs.
- Increase the use of external threat intelligence that helps inform the organization about existing threats and recommended actions.
- Use encryption for any sensitive data, communications or devices.
- Maintain written guidelines and regular training to employees regarding information security risks and responsibilities.
- Perform regular security assessments to determine current state of threats and identify priority patches.

APTs are particularly difficult to deal with because they are often only detected after damage is done. Target's recent data breach, which saw the theft of approximately 40 million credit and debit card numbers and 70 million customer records, was an example of an APT attack. It is estimated that more than 90% of these types of intrusions are discovered through third-party notification.

When dealing with APTs, an organization must consider both strategies for early detection and incident response. Systems should be put in place to monitor the organization's network. These systems are designed to identify anomalies or faint signals that are possible indicators of a problem. Once these anomalies have been detected, an incident response (IR) team must quickly go into action to determine root causes and execute a remediation strategy. A pre-designed and well thought out IR plan should be available to the IR team. Threat intelligence becomes easier for an IR team if its members are trained and can work off an established protocol.

III. CONCLUSION

As said by someone "The threat is advancing quicker than we can keep up with it. The threat changes faster than our idea of the risk. It's no longer possible to write a large white paper about the risk to a particular system. You would be rewriting the white paper constantly..."

To deal with the current environment, we should consider above explain cyber security trends and measures to reduce them. If IT administrators, security and forensics teams don't truly understand the essence of this modern malware, it can easily get in the way of daily tasks and hinder detection, eradication and recovery processes.

IV. REFERENCES

[1] Govil, J.; Michigan Univ., Ann Arbor; Govil, J. Ramifications of cyber crime and suggestive preventive measures Published in: Electro/Information Technology, 2007 IEEE International Conference.

[2] Mathew, A.R. ; Dept. of Inf. Technol., Coll. of Appl. Sci., Nizwa, Oman ; Al Hajj, A. ; Al Ruqeishi, K. Cyber crimes: Threats and protection .

[3] "A federated architecture approach for Internet of Things security" Leo, M. ; Battisti, F. ; Carli, M. ; Neri, A. Euro Med Telco Conference (EMTC), 2014 .

[4] "Optimum tuning of defense settings for common attacks on the web applications" Dwen-Ren Tsai ; Chang, A.Y. ; Peichi Liu ; Hsuan-Chang Chen, Security Technology, 2009. 43rd Annual 2009 International Carnahan Conference.

[5] "A strategic framework for managing internet security" Sitnikova, E. ; Asgarkhani, M. Fuzzy Systems and Knowledge Discovery (FSKD), 2014.

[6] "Security threats in cloud computing" Shaikh, F.B. ; Haider, S. Internet Technology and Secured Transactions (ICITST), 2011.

[7] "Characterizing the Performance of Security Functions inMobile Computing Systems" Rashwan, A.M. ; Taha, A.-E.M. ; Hassanein, H.S. Internet of Things Journal, IEEE Volume: 1 , Issue: 5 .

[8] "Collaboration-Based Cloud Computing Security Management Framework" Almorsy, M. ; Grundy, John ; Ibrahim, A.S.2011.

[9] "Security and privacy in mobile cloud computing" Hui Suo ; Zhuohua Liu ; Jiafu Wan ; Keliang Zhou Wireless Communications and Mobile Computing Conference (IWCMC), 2013.

[10] "An analysis of cloud computing security issues" Behl, A. ; Behl, K. 2012.

[11] http://en.wikipedia.org/wiki/Computer_security.

[12] http://en.wikipedia.org/wiki/Cyber_security_standards.

[13] http://www.gartner.com/newsroom/id/2595015.

[14] http://en.wikipedia.org/wiki/Service-level_agreement.

[15] http://www.mcafee.com/in/resources/white-papers/wp-combat-advanced-persist-threats.pdf.