Understanding Awareness of Cyber Security Threat Among IT Employees

Hamad AL-Mohannadi*, Irfan Awan*, Jassim Al Hamar†, Yousef Al Hamar†, Mohammad Shah‡, Ahmad Musa*
*School of Electrical Engineering and Computer Science
University of Bradford
Email: H.I.M.Al-Mohannadi@student.bradford.ac.uk, I.U.Awan@Bradford.ac.uk, a.s.musa1@student.bradford.ac.uk
*Ministry of Interior, Doha, State of Qatar
Email: j.alhamar@hotmail.com
*University of Liverpool, Liverpool, UK
Email: Yalhamar@hotmail.com
*Knowledge Engineering Ltd., Bradford, UK
Email: shah.shahin@gmail.com

***Abstract*—Cyber-attacks have been an increasing threat on people and organisations, which led to massive unpleasant impact. Therefore, there were many solutions to handle cyber-attacks, including Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS). These solutions will provide a huge number of alarms that produce more are false positives. Therefore, the IDS tool result should be operated by a human intelligent be filtered effectively the huge amount of alerts to identify true positive attacks and perform accordingly to the incident response rule. This requires the IT employees to have enough knowledge and competency on operating IDS, IPS and incident handling. This paper aims to examine the awareness of cyber security threat among all IT employees, focusing on three domains: Knowledge, Monitoring and Prevention.**

Keyword *- Cyber-Attack, Security Awareness, Cyber Threat*

I. Introduction

Information technology is changing the way we do business and communication. Organisations are increasingly depending on information technology to improve their product and quality of services. It is hard to secure personal and organisation data as it can be stolen at any time in any form. European Union has published new data protection regulation called General Data Protection Regulation (GDPR)[1], which aims to protect user data . Following GDPR is not enough for the organisation, they need to train people [1] and build cyber defence [2].

Even a small organisation maintains mailing service to communicate with employees, clients and stake holders. Malicious emails can ruin the reputation of an organisation. Such attack is called phishing attack where an attacker sends spam emails to employees to an organisation pretending to be a genuine one. It is very hard for a employee to make a decision whether to click the link or not. These decisions could be supported by appropriate training about information security awareness. Information security awareness gives the user more understanding about the importance of the best practice. It is important that training is provided to all the employees within organisation [3]. On the other hand, IT employees, who are at the front line of cyber-attack or threat, could cause more harm than others. IT employees' negligence can cost organisation not only money but also valuable data. The threat from the employee may not be always intentional; it could be because of the lack of enough knowledge about cyber risk and consequences. So, it is important to understand the level of knowledge that IT employee have regarding cyber threat in corporate network. Organisations should also look for security awareness services, which can help both employees and organisation understand the weakness of the network.

In this paper, we examine the awareness of cyber-security threat among all IT employee focusing on their Knowledge, Monitoring and Prevention against cyber-attacks. We have collected data from IT employees from various organisations who are responsible to handle cyber security events. The data is collected using interview and questionnaire. This paper also aims to advice a security awareness, which could be adapt depend on the organisation's need and strategy.

II. Literature Review

Cyber-attack is one of the critical issues for most of the organisations. Governments and companies are trying hard to protect valuable data from being stolen. There are a number of systems such as Intrusion Detection System (IDS), Intrusion Prevention System (IPS), firewall, packet shaping devices are around to protect network. There are also a number of attack modelling techniques to support organisation to understand the nature of attack [4]. Protecting the network from external attackers is one of the priorities by the organisations. However, the main issue identified by many researchers in cyber-attack is the employee within the organisation. Employees are the front line of defence of any organisation for protecting the network as well as the biggest threat. Honeypot is used to detect, identify and gather information within the company to reduce cyber risk from the employee, i.e., insider threat [5]. In many occasions cyber-attack happens to an organisation's network because of the lack of knowledge among the employees. Shaw

[1]https://www.eugdpr.org/

et. al. [6] studied on the security awareness and training effectiveness [7]. They have identified that there are a number of barriers in organisation for security awareness, such as budget, computer skills and general security awareness. Cyber security awareness delivery method is important within organisation. Research suggested that combined security awareness is better than individual delivery [3]. Most of the organisations provide basic training to the employees. These training are mostly online base or basic introduction. Security awareness is very useful [8], which could give user more understanding about cyber threat. Along with the training, change of behaviour is important. Phishing attack is very common to any organisation to understand user awareness, which mostly used by the attackers using email. An investigation on the phishing threat on human behaviour is conducted by Nalin et. al. in [9], using mobile game prototype. The result shows a significant improvement on participants to avoid phishing. Phishing for user security awareness exercises is helpful for security awareness [10].

III. Research Method

We have conducted a survey by distributing questionnaire to various cyber threats handling team. The main goal of cyber-attack survey is to support threat hunting as the knowledge and experience of cyber security team is important to mitigate cyber-attack. These teams include a number of different cyber security professionals, who work directly or indirectly in cyber security team. Security Operation Center (SOC) personnel mainly deal with direct cyber-attack to an organisations network. There are some other personnel in the organisation who do not handle or tackle cyber-attack directly but support to mitigate problems.

Data collection will be performed with the full consent of the participant. In this research no personal data will be collected. Also, the aim of the data analysis will focus on the knowledge and awareness of IT employee about cyber threat in their network. The questionnaire will be only sending to people who are directly involved in cyber security or networking.

We have distributed about 50 questionnaires among the participants in different organisations. There were about 22 IT subject matter expert respondents to the survey representing: SOC, NOC, System Admin, Database admin, Network engineer, Application developer, System architect were involved in the survey study. The response is about 44%, which is acceptable for data analysis as questionnaires. The researchers also have profile into two categories: SOC and NON-SOC team. Since combating this risk is the responsibility of all not only SOC but also the Non-SOC team. There were 17 respondents from non-SOC team who are IT Subject matter expert from different domain and only 5 from the SOC team who deal with daily security threats. These expert IT employees, who are expert in their area, have answered the following questions in the questionnaire -

1) In terms of your security duty, do you have a defined checklist for your daily duty?
2) What the common attacks do you handle normally?
3) Do you recognize any of the terms during a cyber-attack?
4) Which of the following Indicator of compromise (IoC) is the most/least difficult to trace in your environment?
5) What are the common alerts do you handle daily?
6) In case of repetitive attacks, what action do you take?
7) Do you have any procedure to follow in case of attacks?
8) Do you use any (firewall, IDS, IPS, router etc.) log data to understand activities in the network?
9) Do you have an operation center to monitor all attacks?
10) Is your workstation/Server implemented using a managed client/server architecture, or in a stand-alone to push the policy configuration and update?
11) Do you have DMZ for external and firewall for internal cross-site?
12) Does it help in isolating or preventing the attack?

These questions are designed as multiple choice question for the convenient of the participant and data analysis. Participants also have the option to answer differently if the desired answer is not in the list.

We have also use interview technique to SOC and cyber security researchers. The following is the questions were asked during the interview sessions -

- What do you do in a normal day?
- What kind of attack do you handle normally?
- Do you recognise any of the components from the following during a cyber-attack
  1) Hash values
  2) IP Address
  3) Domain Name
  4) Network Artefact
  5) Host Artefact
  6) Attack tools (e.g., used same tool before by attacker)
  7) Other special techniques

  Which one is the most/least difficult to trace for supporting the alert system?
- What kind of alert you get?
- If you see same kind of attack happening in your network, what action do you take?
- Do you have any procedure to follow?
- Do you use any (firewall, router etc.) log data to understand activities in the network?
- Do you any operation centre to monitor all attacks?
- Is all the pc/ machine have the same configuration and update in the operation room?
- Are the firewalls are flat or cross site?

IV. Cyber-Attack Survey

We have conducted a survey by distributing questionnaire to various cyber threat handling teams. The aim of these questionnaires is to understand knowledge and awareness of IT security staff. It is important to know how IT security staffs react during an event of cyber-attack.

We have conducted the research on various teams that includes a number of different cyber security professionals, who

TABLE I
KNOWLEDGE OF IT EMPLOYEE

Knowledge Elements	SOC	Non-SOC	Difference
Antivirus/malware	84.9%	90.3%	5.4%
Firewalls	78.2%	90.3%	12.1%
Indicator of compromise (IoC)	68.1%	48.4%	-19.7%
Data encryption (data in transit)	59.7%	61.3%	1.6%
Data encryption (data at rest)	61.3%	48.4%	-12.9%
Patch and vulnerability management	61.3%	41.9%	-19.4%
Intrusion detection system (IDS)	100.0%	41.9%	-58.1%
Intrusion prevention system (IPS)	100.0%	45.2%	-54.8%
Mobile device management (MDM)	56.3%	35.5%	-20.8%
User privilege controls	75.0%	45.2%	-29.8%
Access control lists (ACL)	65.0%	41.9%	-23.1%
Network traffic monitoring tools	85.0%	45.2%	-39.8%
Web security gateway	80.3%	32.3%	-48.0%
Multi-factor authentication	41.2%	32.3%	-8.9%

work directly or indirectly in cyber security team. Security Operation Centre (SOC) personnel mainly deal with direct cyber-attack to an organisation's network. There are some other personnel in the organisation who do not handle or tackle cyber-attack directly but supports to mitigate such problems. The survey has examined the awareness of cyber security threat among employees within the organisation. We mainly focus on three domains of cyber threat intelligence such as

- Knowledge - To identify how much knowledge of an IT employee has for cyber security related tools, techniques etc.
- Monitoring - To understand how the cyber security team perform cyber incident monitoring.
- Prevention - To understand how IT employee prevent cyber-attack events.

A. Survey Result

The result indicates that there is a gap of knowledge between Security operation team and other IT subject matter expert. Interestingly, only 68.1% of SOC team and less than half (48.4%) of non-SOC team are knowledgeable about Indicator of compromise (IoC). Likewise, only 65% of SOC teams are aware or use Access Control Lists (ACL) and 41.9% of non-SOC. Moreover, only 75% of SOC team and 45.2% of non-SOC team are reviewing user privilege access activity. Table I indicate that while SOC team have better knowledge of cyber security threat, non-SOC team show less positive results where most of their score are below 50%. In Figure 1 we intend to explore the capability of the IT employee to identify and safeguard from cyber security threats. The data in Figure 1 shows that SOC team are generally capability of safeguarding from cyber security threats if they are able to identify it. Moreover the greater threats are (Zero-day attacks, malicious insider attacks, Advanced Persistent Threat) attacks which are hard to identify and safeguard from. These types of attacks are advanced and require highly skilled hackers to identify unknown world-wide vulnerability in the victim IT Infrastructure and then plan to get access to the network. However security experts recommend having disaster recovery including business continuity plan to reduce the impact such attack. Result also shows great gap between SOC and non-SOC which need to be narrowed. Security works on number of layer of defence non-SOC is certainly one of them. In

	Soc		Non-Soc		GAP	
	Identify	Safeguard	Identify	Safeguard	Identify	Safeguard
Denial of services attacks (DoS)	7	9	4.6	4.24	-2.34	-4.76
Advanced persistent threat (APT)	4.1	4.1	2	3	-2.15	-1.1
Spearphishing attacks	8	9	4.6	5.21	-3.37	-3.79
Malicious insider attacks	4.1	5.7	4.1	4.71	0	-0.99
Ransomware attacks	6	5.0	4.4	5.02	-1.59	0
Brute force attacks	6.5	7	5.5	5.26	-1	-1.74
Zero day attacks	3.2	4.5	2	2	-1.2	-2.5
Insider attacks	4.7	6	4.7	5.4	0	-0.6
Exploitation of known software	5.2	7	7	9	1.8	2

Fig. 1. Capability to IDENTIFY/SAFEGUARD IT infrastructure

Figure 2 we are looking at methods used by the responders to ensure there ability to identify security threats. Result shows

	SOC	Non-Soc	GAP
Monitoring of system activity logs	76.50%	74.20%	-2.30%
Monitor network traffic	75.60%	22.00%	-53.60%
Monitoring of user access logs	67.20%	15.00%	-52.20%
Use cyber Security threat report	47.10%	32.30%	-14.80%
Search for Vulnerability & Exploit Database	32.80%	16.10%	-16.70%
Working with other team such as (Soc Team)	32.80%	9.70%	-23.10%

Fig. 2. Methods Used to Identify Threats

that each member of IT domain is using some methods to identify threat or check the health of their system. Furthermore only 32.80% of SOC team and 16.10% of non-SOC team are searching in Vulnerability & Exploit Database. This is great risk since it could open a gateway for hacker to access your network or system. Finally, getting SOC and non-SOC team working to gather is a challenge which organizations need to overcome by setting up daily report, weekly meeting to discuss latest challenges related to cyber security threats. Figure 3 demonstrates the process of risk assessment, vulnerability scan, penetration testing knowledge for the SOC and non-SOC staffs. The survey result does not reflect good knowledge among those employees. We have identified that only 31.9% of the SOC team members has good knowledge of penetration test result, whereas only 22.6% of non-SOC staffs is aware of that report. So, this implies that in the area of prevention and proactive response need to improve among the relevant departments who are responsible for mitigating cyber-attack. In Figure 4 we demonstrate the survey result of network security and protection, endpoint protection, disaster recovery, business continuity plan and data loss prevention. The result shows that both SOC and non-SOC staffs have some level of knowledge of these areas of enhancements. On the other

	Soc	Non-Soc	Gap
Results of risk assessment	63.9%	77.4%	13.5%
Results of vulnerability scan	45.4%	35.5%	-9.9%
Reports from 3rd parties about increased cyber attacks	45.4%	32.3%	-13.1%
Results of penetration tester's report	31.9%	22.6%	-9.3%

Fig. 3. Prevention and Proactive Responses

hand, in some areas such as network and security operation and data loss prevention knowledge of SOC is about 50%, which is very low for the team.

	Soc	Non-Soc	Gap
Enhance network security and operation	50.0%	71.0%	21.0%
Enhance endpoint protection	100.0%	67.7%	-32.3%
Enhance disaster recovery (DR)	90.0%	58.0%	-32.0%
Enhance business continuity plan	75.0%	67.5%	-7.5%
Enhance data loss prevention	50.0%	58.0%	8.0%

Fig. 4. Areas of Enhancement

The survey has been conducted among different IT employees, who directly or indirectly handles cyber attack within organisations. The result shows that there is a huge gap of knowledge among those employees regarding cyber attack. Each of the IT team has different level of knowledge about cyber attack. For example, generally, SOC team has got more knowledge on cyber attack than the non-SOC team. It has been noticed that in the case of multi-factor authentication both SOC and Non-SOC team scored very low as 41.2% and 32.3% as demonstration of knowledge. Software patching is one of the important factor for reducing cyber threat and vulnerability. Software patch should be updated on the time of patch released by the vendor. Also, it is important for IT security team to understand patch and vulnerability updates. From the survey it has been noticed that only 61.3% of SOC staff has knowledge of patch and vulnerability management.

V. Security Assessment Services

From the above survey result, it has been noticed that there is a huge gap in knowledge and awareness among IT employees within an organisation. It is important that organisation take necessary steps to build knowledge and awareness about cyber security among the employees. So, we propose some common assessment scenarios that aim to support organisations to keep up to date with cyber security knowledge.

This section describes the of the most common assessment scenarios. These can be customized in many ways to meet organisation's needs. Each type of assessment takes varying amounts of time and is impacted by the number of targets (applications, servers, networks, etc.). The exact type of assessment should be determined in the initial meeting.

A. Network-Based Attack & Prevention

Network-based attack always could cost a lot for an organisation. One of the prominent network-based attack is the denial of service attack, which can be prevented by using design decision [11]. Organisations need to check the vulnerabilities of the network to prevent cyber-attack. Penetration testing includes components of application vulnerability assessment, host vulnerability assessment, and security best practices. This type of test can be performed with or without detailed prior knowledge of the environment. When it is performed without prior knowledge additional steps will be taken to enumerate hosts and applications and to assess the ease with which any outsider could exploit publicly available information or social engineering to gain unauthorized access [12].

An attack and penetration test will answer questions like -

- How vulnerable is the network, host, and application(s) to attacks from the internet or intranet?
- Can an intruder obtain unauthorized access to critical resources?
- Are social engineering techniques effective?
- Are operational controls effective?

This would involve the Information Security Officer (ISO) acting as an attacker and looking at the system as an outsider. The ISO would look for -

- Remotely exploitable vulnerabilities
- Patch levels (OS and Apps)
- Unnecessary services
- Weakness of encryption
- Weakness of authentication

B. Host Based Assessment

This is an assessment of the health and security of given workstation or server. Automated scanning tools (e.g. Nessus[2]) are the primary vehicle for this type of assessment. Additional hands-on inspection may also be necessary to assess conformance to security best practice. This assessment will answer questions like:

- Is patching up to date?
- Are unnecessary services running?
- Are anti-virus/anti-malware signatures up to date?

This would involve the ISO acting as a System Administrator and auditing the system and applications looking for -

- Locally exploitable vulnerabilities
- Patch levels (OS and Apps)
- Access rights
- Security best practices

C. Application

This is an assessment of the functionality and resilience of the compiled application to known threats. This assessment focuses on the compiled and installed elements of the entire system, e.g., how the application components are deployed, communicate or otherwise interact with both the user and server environments. Application scanning tools as well as manual testing with and without application credentials are used to perform this assessment. Typically some host, network,

[2]https://www.tenable.com/

and general information security practices are assessed as part an application vulnerability assessment.

This assessment will answer questions like -

- Does the application expose the underlying servers and software to attack
- Can a malicious user access, modify, or destroy data or services within the system

This would involve the ISO auditing an application (typically web based) and looking for vulnerabilities like -

- SQL Injection
- Cross Site Scripting
- Cross Site Request Forgery
- Improper data sanitization
- Buffer overflows (limited)
- Misconfigured or weak authentication

D. Compliance

This would involve the Information Security Office auditing (or assisting in the coordination of an audit if the ISO is not trained to conduct the specific audit) systems for compliance with specific regulations:

- GDPR
- HIPAA
- FERPA
- GLBA
- PCI

E. Physical Security Assessment

This assessment typically involves interviews with key staff, documentation review, and an on-site visit to assess appropriate physical and environmental controls for safeguarding computing resources.

This assessment will answer questions like -

- Are there appropriate physical access controls in place for securing servers and desktop machines
- Are appropriate environmental controls in place to sustain critical computing infrastructure
- Are systems left logged in while staff are away

VI. Conclusions

The result shows that the IT employees need to improve their knowledge in many aspect of cyber threat. It indicates that there is a gap of knowledge between Security operation team and other IT expert which need to be narrowed. SOC team are generally capability of safeguarding from cyber security threats if they are able to identify it.

The Methods Used to Identify Threats were mainly through monitoring tools and less attention were given to Security threat report, vulnerability assessment, and communication and cooperation with the SOC and non-SOC team.

Moreover, participants including the SOC and non-SOC operate show insufficient knowledge on the practice of risk assessment, vulnerability assessment and penetration testing. Both participants agreed on the need for enhancing data loss prevention. It should be mandatory for all the IT employees, who work directly or indirectly on cyber-attack must have advanced training. In this paper, we also recommend security assessment service to support ISO. Security assessment service provides guideline to prevent network, host, application and physical security. This is the combination of both human and machine, which need to follow rules and regulations. For example, organisations must follow the GDPR to protect both the user and themselves. Also, they need to maintain physical security of the network and any individual hosts. So, it is important to do periodic penetration testing across the network to find the vulnerability.

In the future work, we aim to perform more survey research on other organisations to get reliable results on the average awareness of IT employees on cyber security. It is recommended to use another method to assess employees knowledge on cyber security through penetration testing, observations and simulation. To reduce the gap of knowledge between Security operation team and other IT expert it is suggested for a future work to enhance communication between both teams throu gh regular meetings and to provide a scheduled transfer knowledge sessions on specific knowledge including cyber security. Also, providing specialized training on cyber security or awareness sessions would be beneficial to ensure that all IT employees absorbed the required knowledge on cyber security and on how to handle such incidents effectively.

References

[1] E. Albrechtsen and J. Hovden, "Improving information security awareness and behaviour through dialogue, participation and collective reflection. an intervention study," *Computers & Security*, vol. 29, no. 4, pp. 432–445, 2010.

[2] M. Golling and B. Stelte, "Requirements for a future ews-cyber defence in the internet of the future," in *Cyber conflict (ICCC), 2011 3rd international conference on*. IEEE, 2011, pp. 1–16.

[3] J. Abawajy, "User preference of cyber security awareness delivery methods," *Behaviour & Information Technology*, vol. 33, no. 3, pp. 237–248, 2014.

[4] H. Al-Mohannadi, Q. Mirza, A. Namanya, I. Awan, A. Cullen, and J. Disso, "Cyber-attack modeling analysis techniques: An overview," in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, Aug 2016, pp. 69–76.

[5] L. Spitzner, "Honeypots: Catching the insider threat," in *Computer Security Applications Conference, 2003. Proceedings. 19th Annual*. IEEE, 2003, pp. 170–179.

[6] R. S. Shaw, C. C. Chen, A. L. Harris, and H.-J. Huang, "The impact of information richness on information security awareness training effectiveness," *Computers & Education*, vol. 52, no. 1, pp. 92–100, 2009.

[7] M. Wilson and J. Hash, "Building an information technology security awareness and training program," *NIST Special publication*, vol. 800, no. 50, pp. 1–39, 2003.

[8] K. J. Knapp, T. E. Marshall, R. K. Rainer Jr, and F. N. Ford, "Information security effectiveness: Conceptualization and validation of a theory," *International Journal of Information Security and Privacy (IJISP)*, vol. 1, no. 2, pp. 37–60, 2007.

[9] N. A. G. Arachchilage, S. Love, and K. Beznosov, "Phishing threat avoidance behaviour: An empirical investigation," *Computers in Human Behavior*, vol. 60, pp. 185–197, 2016.

[10] R. C. Dodge Jr, C. Carver, and A. J. Ferguson, "Phishing for user security awareness," *computers & security*, vol. 26, no. 1, pp. 73–80, 2007.

[11] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the dos and ddos problems," *ACM Computing Surveys (CSUR)*, vol. 39, no. 1, p. 3, 2007.

[12] B. Arkin, S. Stender, and G. McGraw, "Software penetration testing," *IEEE Security & Privacy*, vol. 3, no. 1, pp. 84–87, 2005.