SECURING THE HUMAN TO PROTECT THE SYSTEM: HUMAN FACTORS IN CYBER SECURITY

*M.G. Lee**

**Symantec.cloud,1240 Lansdowne Court ,Gloucester.GL3 4AB. Email: martin_lee@symantec.com*

Keywords: information security, human error.

Abstract

Analysis of the publications of the Information Commissioner's Office relating to prosecutions or monetary penalties for data breaches shows that many of these breaches involved human error. The most common such errors in these reports are well meaning insiders making slips in routine operations. Technical correction strategies to mitigate against the error were either absent or ineffective in preventing harm from being incurred. This paper considers the failure modes of human operators of information systems within reports issued by the Information Commissioner's Office. These demonstrate where additional technological assistance may be better directed to reduce probability of occurrence and to reduce the impact of information security failures.

1 Introduction

Learning from the past is an important component of engineering practice. In the UK various statutory bodies have the legal duty to investigate incidents where safety has been compromised. These investigations publish the findings of the steps that led to the incident, and recommend how similar future incidents can be avoided, or the effects minimised. This work has resulted in a large body of knowledge from which engineers can learn and improve local practice.

The advance of technology allows the construction of new systems that perform new tasks. However, due to a lack of experience, or knowledge, occasionally these systems fail in ways that the designers failed to predict. Thorough investigation and consideration of the failure modes of emerging technology allows mitigation strategies to develop that are effective in preventing these failures from reoccurring.

1.1 Information Security

The requirement to maintain the confidentiality of certain information has been recorded since the era of classical Greece. Tattooing a message on the shaved scalp of a slave then concealing it under the re-growth of hair kept the information safe from unauthorised disclosure [1]. However, the growth of information produced by organisations, facilitated by developments in information technology, requires a different approach to maintaining information security. It is estimated that 1.8×10^{21} bytes of data was created during 2011, a nine fold increase over 2006 [2]. This data requires some degree of security protection. The commonly accepted means through which information security is achieved, is by assuring the confidentiality, integrity and availability of information [3]. Incidents where the required level of security is breached can have severe consequences for organisations.

1.2 Consequences of Breaches

Breaches of information security can cause quantifiable financial harm. Anecdotal reports of high profile breaches suggest that incidents may cost tens of millions of dollars to resolve [4][5]. Broader industry surveys suggest that breaches resulting in the loss of personal data cost, on average, $5.4 million per incident [6]. However, other studies suggest that the financial impact of most security incidents is much lower. The PWC Information Breaches Survey finds that the average cost of an organisation's worst security breach for a year ranges from £15k - £30k, for small organisations, to £110k - £250k for large organisations [7].

Part of the disparity between such figures may be that there is no commonly accepted framework by which to measure the financial impact of information security incidents. Indirect costs, such as damage to reputation, may account for a large proportion of the total financial harm. However, this is difficult to quantify, and in any case, organisations may be unwilling or unable to calculate such figures [8].

1.3 Protection from Harm

To avoid the consequences of information security incidents, organisations must deploy suitable defences to protect their systems. Comprehensive lists of suitable defences are published, such as that from NIST [9]. Each control successfully implemented increases the chances of detecting and neutralising attacks or mitigating against the harm that may result from successful breaches of security. However, organisations must select the defences which are appropriate to their circumstances, have the means to deploy the defence and to assure its continuing effectiveness.

The defences deployed to protect an information system must take into account the users of the system and their needs. System users will have their own goals to achieve in their usage of the system and may not necessarily use the system in the ways imagined by the designers [10]. This may expose the system to new threats for which defences are inadequate, or anticipated threats may never be encountered. How should system designers be sure that they are deploying the correct protective measures against the correct threats?

One means by which system designers may learn of the types of threats that they will encounter is to study reports of failures in other similar systems. However, organisations may be unwilling to disclose reports of breaches due to negative market perceptions, which can cause measurable drops in market capitalisation [11][12]. Alternatively, organisations may find that the costs of investigating and reporting breaches are too high to produce incident reports [13].

1.4 Human Failure Modes

One way in which systems may fail, is through the incorrect action of the system's operators. System safety researchers have a long history of investigating safety failures and understanding the *slips*, *lapses*, *mistakes* and *violations* of human behaviour that have led to the failure. While every incident is unique, human behaviour tends to conform to certain patterns. Understanding these patterns in the context of a safety failure, or a data breach, allows the elucidation of where further protective measures can be better deployed to support human operators and to reduce the possibility of a safety failure or data breach occurring [14].

Familiar, routine tasks are often performed by humans as a skill with little conscious effort. Errors made at this level of operation are known as *slips*, where the wrong action is performed, or *lapses*, where actions within a task are omitted or the correct actions are performed but in the wrong order [15].

More complex tasks that fall outside of the routine may be performed according to learnt rules that express how tasks should be performed correctly. Such tasks require more conscious thought than skill based tasks, and involve the correct interpretation of the task and the situation in which it occurs. Selection of the wrong rules to perform tasks are known as *mistakes* [15].

Complex tasks that are not easily performed according to pre-learnt rules can be achieved according to knowledge based performance. This may require significant mental effort and creativity in order to perform the task satisfactorily. Errors at this level of operation where the wrong course of action is taken are also known as *mistakes* [15].

A further class of errors occurs where a human makes a decision to deviate from accepted procedure and chooses a different course of action. These errors are known as *violations* [15].

In some cases, the cause of the failure or breach may be someone who does not have permission to access the system, an *outsider*, who may be acting with malicious intent rather than an authorised operator acting in error but with good intentions. Adverse outcomes can also be caused by well meaning operators following the accepted procedure to the letter. In these cases it is the procedure that is at fault. Such latent errors in procedures may remain undetected for many years until certain conditions are experienced which cause the error to become manifest [16].

2 Methods

To determine how human actions may lead to data breaches the publications of the Information Commissioner's Office of the United Kingdom (ICO), were analysed [17]. The ICO, among other responsibilities, can take action to enforce data privacy laws. As part of this, the ICO may publish notices of the enforcement action that it has undertaken. The news releases relating to successful prosecutions and published monetary penalty notices contain a narrative description of the events that led to the ICO taking action. The analyses of these publications were aggregated to determine the most common human failures that lead to information security breaches.

The publications were analysed to determine if the described breaches were caused by the actions of individuals who were *insiders* or *outsiders* to the organisation. An *insider* being defined as an individual who is acting under the instruction of the owner of data, such as employees and contractors. An *outsider* being defined as any other individual. The action of the individual was ascribed to be *well meaning*, if the individual concerned appeared to believe that they were acting in the interests of the data controller, or that they were acting according to local policy. The action was ascribed to be *malicious*, if the perpetrator appeared to be wilfully acting against the interests of the data controller.

Publications were also analysed to determine if the breach was caused by a *slip*, *lapse*, *mistake*, *violation*, or if the system was in compliance with local policy at the time of the breach.

3 Results

27 reports were analysed from the ICO website [17]. These comprised 7 notices of prosecutions dating from 1 June 2011 to 30 March 2012, and 20 monetary penalty notices dating from 22 November 2010 to 5 July 2012.

These published incidences are not necessarily representative of all data breaches. Only the most egregious contraventions are likely to be investigated, many transgressions may go unnoticed and unreported. Nevertheless these reports represent a collection of data breaches deemed important enough to warrant investigation by an independent third party.

Insiders were responsible for the majority of data breaches reported rather than outsiders.

Actor	*Incidence*
Insider	17/27 (63.0%)
Outsider	10/27 (37.0%)

Table 1: Position of the individual causing the data breach.

Of the insiders, the majority were well meaning.

Actor	*Incidence*
Well meaning insider	12/26 (46.2%)
Malicious insider	3/26 (11.5%)
Malicious outsider	11/26 (42.3%)

Table 2: Intention and position of the individual causing the data breach.

In one case it was not possible to ascertain if the individual involved in the breach was acting maliciously or was well meaning [18].

Within the incidents that were deemed to involve individuals acting maliciously, it is important to note that one of these incidents did not result in an actual data breach, but did result in a successful prosecution. In this case the application of local procedure correctly identified an attempt to access data by an outsider acting maliciously [19]. One additional press release relating to a prosecution did not detail how the data breach occurred beyond that the incident appeared to involve an insider [20].

Within the reports involving malicious intent, only 7 could be judged to clearly involve a violation of local policy and procedures. In 5 cases, the data breach incidents appeared to occur while complying with local policy, 3 of these incidents concerned the theft of devices containing unencrypted personal data.

12 reports involved well meaning insiders. 9 of these were judged to be due to slips where a minor error was made in following local procedure. 3 were judged to be due to mistakes. The mistakes occurred where local procedure did not appear to cover the situation encountered. The operator faced with this situation apparently chose a course of action based on their knowledge and understanding. Nevertheless, this course of action ultimately appeared to lead to a data breach.

Taken together the data show that the most common human error involved in this set of reports of data breaches is due to well meaning insiders making slips in routine operations. The next most common class of incident is the actions of malicious outsiders causing data breaches while the data and systems it resides in are being held in compliance with local policy.

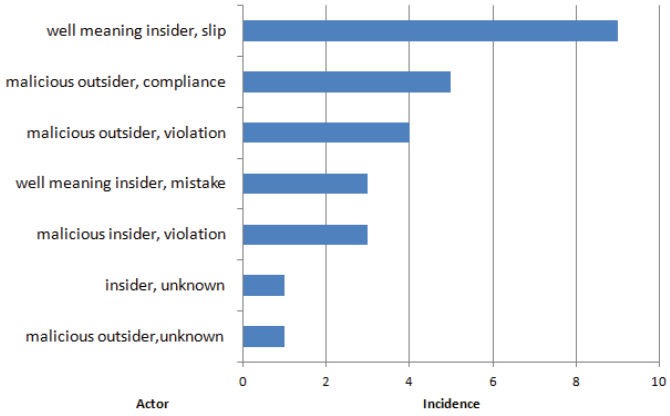

Figure 1: Intention, position and class of human error involved in information breaches.

4 Discussion

Much debate regarding the subject of cyber and information security tends to concentrate on the threats posed by malicious outsiders. Such actors can cause great harm to organisations, but insiders may pose a greater risk. The nature of the malicious insider risk is well recognised. Insiders are well placed to cause harm to organisations due to their trusted nature and detailed knowledge of systems and procedures [21].

Malicious insiders must remain the exception; if every insider was malicious, no organisation could function. It can be assumed that given the opportunity, most employees will diligently perform the tasks assign to them to the best of their abilities. However, it must be recognised that this poses its own risks, in that human beings are prone to human error. This analysis of data breach reports finds that within the reports from the ICO that resulted in prosecution or the issuing of a monetary penalty, the most common reason for a data breach was a slip, a deviation from correct procedure in a task, performed by an insider without malicious intent.

Slips in tasks can be anticipated and systems designed to detect such slips to correct them before harm is caused. Data loss prevention systems can act to ensure that data is managed in compliance with local policy and to alert administrators to breaches in policy, whether this is due to slips, mistakes or violations. Nevertheless, this requires policy to be actively monitored and enforced. A well designed encryption protocol for data can help to ensure that only authorised individuals or recipients are able to decrypt and access data, thus rendering it difficult to turn a casual slip into a data breach. In these ways, local policy can be upheld, but again, administrators must monitor and enforce policy to ensure that valuable data is correctly encrypted.

To be effective, the system upholding local policy can only protect data if the local policy provides adequate protection. The number of data breaches involving malicious outsiders where the data has been breached even though it was

apparently being handled in compliance with local policy suggests that setting of correct policy may be a problem for organisations. A policy that does not anticipate relevant threats may consume resources and time in ensuring compliance, but these resources will be wasted if the policy is not actually mitigating against the encountered threats.

Three of these incidences concerned theft where an employee was off premises with work data with the apparent intention of continuing to work. This was either in compliance with local policy, or without relevant policy apparently being in place. In these cases the policy did not provide suitable protection, possibly because it failed to consider how users would need to access data to fulfil their tasks.

Those responsible for the protection of data, the data controllers, need to consider how slips made by operators may be detected and rectified before data is breached. Additionally, data controllers need to consider how people may be using and accessing data outside of the scope of the original system design. This is especially true as technological or societal change affects how people perform their work duties, such as using personal devices for work purposes, or increasingly working remotely outside of the traditional office boundaries.

5 Conclusion

Cyber-security is often considered as protecting data and systems from external attack. Analysis of the published decisions of the ICO shows that 44.4% of these are due to slips by well meaning insiders. Operators use systems and data to perform their day to day tasks. However, like all humans, these operators are prone to human error. System architects need to take into consideration how slips can be detected and corrected to prevent harm from occurring.

42.3% of incidents were due to the actions of malicious outsiders; the majority of these cases occurred when the data that was breached was held in compliance with local policy. In these cases, the policies that had been implemented and the protections deployed to enforce the policy were inadequate. This may be due to system designers failing to anticipate certain types of threats, or failing to anticipate how the systems would be used in practice by users.

System designers must consider how humans may use a system and how these human users may fail even without any malicious intent. Protection needs be deployed not only to protect against external adversaries, but also to secure the fallible humans who use the system. Additionally, designers and system policy managers need to ensure that they understand how systems are being used and how this use is evolving in order to ensure that the security of data is being assured.

Acknowledgements

Thanks to Steve White, Paul Wood and Alistair Johnson for their continued support, and to Wendy Goucher for her encouragement in the preparation of this paper.

References

[1] D. Kahn, “The history of steganography”, in *Lecture Notes in Computer Science,* pp. 1-5, (1996). DOI: 10.1007/3-540-61996-8_27

[2] J.Gantz, D. Reinsel “Extracting Value from Chaos”, *IDC Iview Report*, (2011). http://idcdocserv.com/1142

[3] M.E.Whitman, H.J. Mattord, “Introduction to information security”, in *Principles of Information Security 4th Edition*. pp. 1-35, (2012). ISBN-13: 978-1-111-13821-9

[4] H.Tsukayama, “Cyber attack on RSA cost EMC $66 million”, *The Washington Post,* 26th July (2011). http://www.washingtonpost.com/blogs/post-tech/post/cyber-attack-on-rsa-cost-emc-66-million/2011/07/26/gIQA1ceKbI_blog.html

[5] J. Vijayan, “Heartland breach expenses pegged at $140M -- so far”, *Computerworld*, 10th May (2010). http://www.computerworld.com/s/article/9176507/Heartland_breach_expenses_pegged_at_140M_so_far?taxonomyId=17

[6] Ponemon Institute, “2011 Cost of Data Breach Study United States”, *Ponemon Institute Research Report*, (2012). http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf

[7] PricewaterhouseCoopers LLP, “Information Security Breaches Survey Technical Report”, *PricewaterhouseCoopers Report*, (2012). http://www.pwc.co.uk/en_UK/uk/assets/pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf

[8] R.Anderson, C.Barton, R.Bohme, R.Clayton, M.J.G. van Eten, M.Levi, T.Moore, S.Savage, “Measuring the Cost of Cybercrime”, in *Proceedings of the 11th Annual Workship on the Economics of Information Security*, (2012).

[9] National Institute of Standards and Technology, “Recommended Security Controls for Federal Information Systems and Organizations”, *NIST Special Publication 800-53 revision 3*, (2009).

[10] A.Beautement, M.A.Sasse, M.Wonham, “The compliance budget: managing security behaviour in organisations.” in *Proceedings of the 2008 Workshop on New Security Paradigms*, pp. 47-58, (2008). DOI: 10.1145/1595676.1595684

[11] K.Campbell, L.A.Gordon, M.P. Loeb, L.Zhou, "The economic cost of publicly announced information security breaches: empirical evidence from the stock market", *Journal of Computer Security,* **11**, pp. 431-448, (2003).

[12] A.Acquisti, A.Freidman, R.Telang, "Is There a Cost to Privacy Breaches? An Event Study", in *Proceedings of the Twenty-Seventh International Conference on Information Systems,* (2006).

[13] T.M. Lenard, P.H. Rubin, "Much Ado about Notification", *Regulation*, **29**(1), pp. 44-50, (2006).

[14] J.Rasumussen, "Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models", *IEEE Transactions on Systems, Man, and Cybernetics*, SMC-13, no. 3, pp. 257-266, (1983).

[15] J.Reason, "Human Error", pub. Cambridge University Press, (1990). ISBN-13: 978-0521314190

[16] J.Reason, "Managing the Risks of Organisation Accidents", pub. Ashgate Publishing, (1997). ISBN-13: 978-1840141054

[18] ICO Monetary Penalty Notice, Brighton and Sussex University Hospitals NHS Foundation Trust, 28th May 2012. http://www.ico.gov.uk/what_we_cover/taking_action/~/media/documents/library/Data_Protection/Notices/bsuh_monetary_penalty_notice.ashx

[17] ICO, "Taking action: data protection and privacy and electronic communications", retrieved 10th Jul 2012. http://www.ico.gov.uk/what_we_cover/taking_action/dp_pecr.aspx

[19] ICO News Release, "Letting agent unlawfully tried to access tenant's benefit details", 27th Feb 2012. http://www.ico.gov.uk/news/latest_news/2012/letting-agent-unlawfully-accessed-tenants-benefit-details-27022012.aspx

[20] ICO News Release, "Gambling worker guilty of selling 65,000 bingo players' details", 10th Nov 2011. http://www.ico.gov.uk/news/latest_news/2011/gambling-worker-guilty-of-selling-65000-bingo-players-details-10112011.aspx

[21] S.L.Pfleeger, J.B.Predd, J.Hunker, C.Bulford, "Insiders Behaving Badly: Addressing Bad Actors and Their Actions", *IEEE Transactions on Information Forensics and Security*, **5**, pp 169- 179, (2010). DOI: 10.1109/TIFS.2009.2039591