thalesgroup.com

THALES

9 factors
reducing insider threat and enhancing cyber security

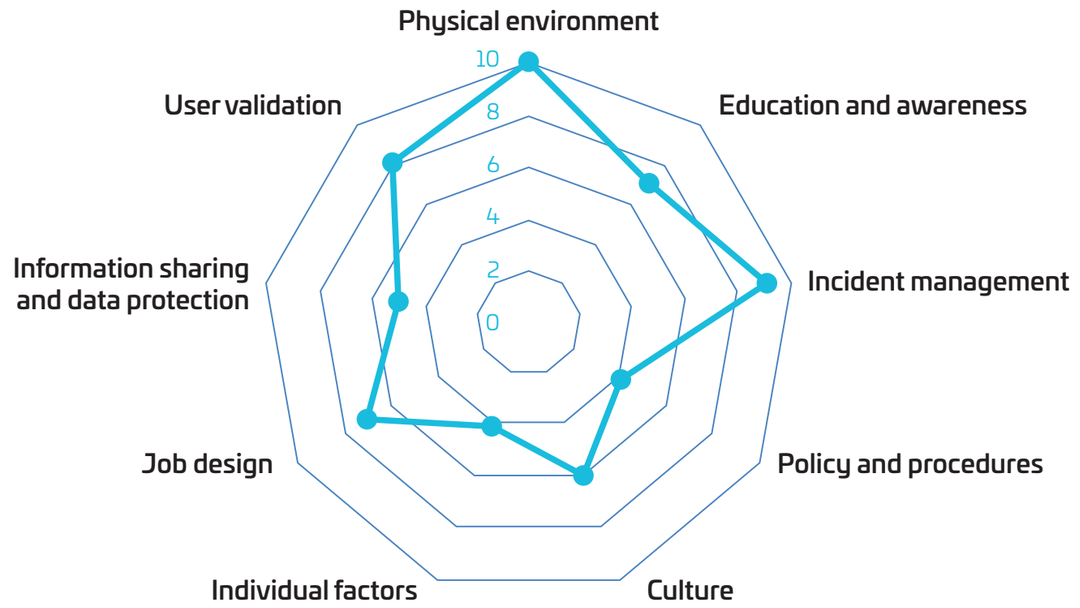
9 factors

reducing insider threat and enhancing cyber security

Reports suggest the majority of cyber security incidents are caused by employees. I present 9 human factors which can be addressed to reduce the risk of insider threat.

Introduction

Insider threat, or the human element, reportedly accounts for the majority of cyber security incidents. This suggests that technical control systems alone are not sufficient to address cyber security risk. Similarly, the majority of insider threat incidents are unintentional, so a focus on the motivations of a malicious attack would also be insufficient. We need to understand non-malicious human limitations and causes of cyber security incidents. This whitepaper describes 9 factors which have been tried-and-tested to reduce insider threat.



1. Policy and Procedures

If cyber security policy is too strict, people will find workarounds. For example, if security procedures make it too difficult to share information with third parties, employees may be tempted to use their personal email or a USB device, thereby creating vulnerability and rendering the technical controls redundant. Rather than punish this behaviour, we should accept it as 'human nature' and make the most secure way, the easiest way. In order to do this, we need to design policy and procedures around people's jobs. This means talking to them and really understanding how the procedures will affect their work. The additional benefit is increased buy-in. Policies and procedures also need to be succinct, easily accessible and endorsed by senior management.

2. Information sharing and data protection

As well as the loss of information through bypassing security policies, use of social media creates vulnerability. Employees may share too much information about sensitive work projects on chat groups and other forms of social media. A malicious attacker could amalgamate location and project information from multiple posts, to build a comprehensive picture which could jeopardise the organisation. The information could also be used to facilitate spear phishing/whaling attacks, where individuals are targeted because of their position and access to information. These attacks use information that is relevant to the target's work, in order to appear more genuine. A successful phishing attack would likely give an attacker access to login and password information, which could allow them to take control of services, for example. Employees who use social media as a platform to complain about their employer could make themselves attractive targets for a social engineering attack. Here, a malicious outsider would persuade them to leak information about their employer. We can address these vulnerabilities by monitoring and open source intelligence surveys.

3. Culture

Culture refers to shared perceptions and behaviours. An organisation's cyber security culture can be measured by several factors. One of the most important of these is whether managers lead by example or 'walk the talk'. It is not enough to tell people they should follow cyber security procedures and best practice. It is also necessary to be seen to perform those behaviours. If the perceived message is 'job performance and productivity are more important than cyber security', the cyber security policy will be undermined. Reward mechanisms need to address cyber security behaviours, as well as productivity.

The policy needs to be endorsed by senior management, and the first level of management has been seen to be most effective in shaping culture. If the policy warns against clicking on hyperlinks in emails, but internal corporate emails regularly ask employees to click on hyperlinks, the policy is undermined and it is more difficult for people to recognise a malicious email. Therefore good cyber security behaviours need to be consistently exhibited throughout the organisation.

Investment in cyber security is also important. This affects the quality of the technical cyber security controls, and the training of employees including information security personnel.

Experience has shown that employees can have a tendency to trust their IT department to protect them from a cyber attack. This allows them to absolve themselves of responsibility for cyber security. In a mature culture, all individuals have ownership of cyber security.

Employee engagement surveys can be adapted to identify culture and engagement regarding cyber security. These work best when combined with interviews and/or focus groups in an organisational transformation programme. This approach can also be used to identify emotional support mechanisms for employees.

4. Physical environment

Networks and sensitive information can be compromised by unauthorised access to the physical working environment. This can be achieved by 'tailgating'; following an authorised member of staff through the entry points. Politeness and the tendency to hold doors open for others, is a human vulnerability in the context of security. This can be mitigated by automatic turnstiles and/or intermittent presence of trained, uniformed security personnel at entry points.

If employees are used to seeing people they don't know in their working environment, they are less likely to challenge an attacker who has gained unauthorised entry. Good visitor management policy can address this. Visitors should be obvious to employees, for example, by the badge they are assigned.

Once inside a building, an attacker will target paper-based information and electronic networks. This can be mitigated by good house-keeping, an enforced clear-desk policy, provision of lockable storage, printer management and encouraging employees to lock their computers when they leave their desks.

The security implications of mobile, remote and lone-working also need to be considered. Encryption techniques and information storage can mitigate the risks.

5. Job design

Cyber security procedure design needs to consider the impact on job performance, as described above. Job factors can also affect vulnerability. For example, frequent time pressure could affect susceptibility to phishing emails. As well as email management advice, the reliance on email as a means of communication could be challenged.

Poor design of equipment and software can increase the risk of error, in particular for information security personnel. This can be alleviated by an ergonomics assessment and factoring security in equipment design.

In accordance with good data protection practice, sensitive information should be separated so that individuals only have access to the information they need to do their work. Jobs should be assessed to identify any cyber security workarounds and associated actions.

6. User validation

A common cyber security policy violation is writing down passwords or storing them in a mobile phone. We all have multiple passwords to remember in our personal and professional lives. It is simply beyond human memory capacity to recall that many different, complex passwords. Whilst this is a deliberate policy violation, it is not usually malicious; the intention is not to cause a cyber security incident. A cyber security policy which requires users to remember complex, automatically-generated passwords, which frequently change, is vulnerable. Therefore, password safes or alternative means of user authentication, such as biometrics (e.g. facial, iris or fingerprint recognition) are advisable.

7. Education and awareness

Cyber security training programmes should incorporate example attacks that are relevant to the target audience. They need to understand the vulnerabilities specific to their work and believe that an incident could happen to them. Phishing email recognition and visitor management training should be included. An organisation should be able to measure how many employees have received cyber security training and understand their level of competence. The competence of information security personnel should also be assessed and monitored.

8. Individual factors

A successful cyber attack only needs one employee, so we need to consider individual factors. Certain personality types are more vulnerable to cyber security. For example, someone with a high degree of social compliance might be more likely to share passwords or hold doors open. An individual's sense of duty affects how well they are likely to follow cyber security procedures. Existing personality tests are often used as part of recruitment, but they could also be used to profile cyber-security related facets.

Whilst personality can account for individual differences, arguably we are all susceptible to cognitive bias. For example, a context bias could explain susceptibility to spear phishing. The attacker uses information relevant to the context of that individual to make the email appear genuine. This information could refer to a recent conference they attended or a known technical interest, for example.

It is important to recognise that an individual's emotional state is likely to change over time. After recruitment, they may incur personal, or job-related, circumstances that increase their desire to support a malicious attack or information leak. Assessment of engagement and support mechanisms is therefore necessary to determine the level of this type of risk.

9. Incident management

It should be easy for employees to report cyber security incidents, and a blame culture should be avoided. Cyber security incidents and near misses should be captured, and identified lessons, put into practice. Best practice would ensure the human factors described above are considered as part of each investigation. A competent human factors expert can support this. The investigation should consider mitigating factors such as those described above – training is not the only solution.

About Thales

Trusted by the military and governments around the world, Thales has the people, processes and technology to reduce risk, improve security and protect your organisation. As you would expect from Thales, the precise service that we provide to each of our clients is tailored to specific needs and always held in the strictest confidence. Our cyber security experts and behavioural analysts will give you:

- A comprehensive Human Factors cyber security audit and evaluation;
- Access to an extended team of specialists with expertise in relevant fields;
- The facts you need to make informed decisions;
- A fast, cost effective, low-risk solution;
- Peace of mind through enhanced security.

About the Author

Amanda Widdowson is an experienced Human Factors consultant and manager, professionally recognised to the highest level; a Fellow of the Chartered Institute of Ergonomics and Human Factors and Associate Fellow of the British Psychological Society. In 2018 she received the CIEHF's Otto Edholm award for "significant contributions to the application of ergonomics/HF". For nearly 25 years, she has applied the full range of HF sub-areas, mostly in the Defence and Rail sectors. Her experience as a human error analyst in rail safety incident investigations and role at Thales allowed her to develop an innovative approach to capture the human element in cyber-security scenarios; the Cyber Human Error Assessment Tool (CHEAT®). This repeatedly tried-and-tested approach can be applied proactively or post-incident and has attracted international interest.

THALES

350 Longwater Avenue
Green Park
Reading
RG2 6GF
United Kingdom
T: +44 (0) 118 943 4500

> thalesgroup.com <