7. Human Factors

People are regarded as the weakest link in cybersecurity.

In this chapter we will aim to cover the primary ways in which human factors are frequently either the root cause or a substantial contributor to cybersecurity failures.

As part of a university lecture, I performed an analysis of the security technologies that existed in 2000, those available in the present day, and those expected to be in place by 2025. The common thread throughout was that although security improves in response to evolving threats, there remains one consistent way to bypass this security – all you have to do is compromise or misuse the valid access of an authorized user.

While it may be possible to fully secure a transaction so that only a valid, authorized person can conduct it, an attacker can still bypass these controls by simply influencing or coercing the authorized individual to perform the necessary actions on his or her behalf.

Manipulating people to do certain things is not the only human factor that can create security gaps. The most significant human factors are:

- **Inadequate cybersecurity subject knowledge** leading to the presence of large amounts of open vulnerabilities.
- **Poor capture and communication of risks** leading to repeated, unanticipated cybersecurity failures.
- **Culture and relationship issues**, both in the enterprise itself and/or in key suppliers, creating disinterested and disaffected personnel with insider knowledge.
- **Under-investment in security training** resulting in a low level of awareness about the security risks we all manage (even if we are not cybersecurity experts).
- **Using trust instead of procedures**, especially for personnel with privileged access to information, systems or devices.

- **Absence of a single point of accountability**. When more than one person is accountable, nobody is.
- **Social engineering**, which can involve various methods of leveraging insiders' access or knowledge to create opportunities that bypass other security controls. These methods may include picking up information from personnel through traditional espionage techniques or manipulating them to do specific things.

The case studies in this book were chosen because I know from experience that they represent the same blend of factors that are typically present in the largest cybersecurity failures. It is no coincidence that each one contained a number of human factors that contributed to the cybersecurity breach.

Before we look more closely at each of these areas, I would like to share some real-world examples of how problems with human factors are easy to detect and therefore easy to take advantage of.

If an organization has poor cybersecurity, people inside and close to it know and talk about it. It is incredibly easy for a cybersecurity professional to find out how strong or weak an enterprise's cybersecurity posture is using only a few, difficult to avoid, questions in any social setting.

After a 2-day onsite security audit at a supplier's place of business, I was once asked the following question by their Chief Information Security Officer:

'We had a full, month-long internal audit a short time ago. They sent 3 people in for nearly 6 weeks. What I would like to ask is this. You were here, alone, for just over 2 days and you not only found everything they did but also some valid items that they missed. We could have saved ourselves a lot of time and money. But what I want to know is – How did you do it?'

I thought for a few seconds about whether or not to reveal the secret. I decided that with the audit over, I could.

'Body language,' I replied.

I had my full list of checks to go through, but 2 days never allowed me much time to test many of them in any depth. I would run through the checks in interview-style meetings with company personnel, and the second the body language around the table showed signs of discomfort, I knew to dig.

The larger the group of people that the company brought along to the meeting, the easier the audit became. I recall that one audit in the Philippines held the record for the most attendees; partly, I think, due to the contract size involved, they brought 28 people to the audit room.

In fact, there was a larger secret I had not revealed. Culture. In organizations with a positive culture that focuses on bettering the staff, people tend to like each other more and get along better. If a problem emerges in such companies, people bring it up and sort it out. Organizations with an employee-oriented culture that values effective teamwork tend to have fewer security gaps and problems.

I was also able to assess and test the effects of organizational culture on cybersecurity in reverse, since I was often called in to audit an organization after some kind of significant failure. In all cases, without exception, there were significant, contributing human factors that resulted from a negative culture. The security gaps often resulted from factors as simple as placing too much work on to too few people, creating stress, or bypassing, ignoring or just not putting security controls in place.

Inadequate cybersecurity subject knowledge

Although cybersecurity relies on some traditional security principles, it also has many new requirements. The speed at which emerging technologies are adopted continuously creates more potential cybersecurity vulnerabilities.

It is not humanly possible to stay on top of the emerging threats and attack vectors unless you dedicate a substantial amount of time to continuous learning.

As a cybersecurity management specialist, I spend around 30% of my professional time reading and learning about new technologies and threats. Although this allows me to keep up with the main risks, there are frequent occasions when I have to go and research a new technology or threat type.

Cybersecurity is not a static discipline that can be learned and applied for years. An ongoing and substantial personal investment is required to stay on top of the subject area.

If a manager does not require his or her cybersecurity staff to hold and maintain current certifications from a recognized authority, he or she will inevitably have issues with the staff's level of cybersecurity knowledge.

The only thing more dangerous than training a cybersecurity employee who may then leave is not training the employee and having him or her stay.

One of the most frequent mistakes I have witnessed between 2015 and 2017 is that many organizations have a tendency to employ a small number of very high cost specialists and then deprive them of the necessary training time to keep their knowledge current.

Poor capture and communication of risks

Chapter 12 is dedicated to this important subject area. There are, however, human factors to consider in any discussion of how risks are captured and communicated.

People often notice risks that can create substantial damage to an organization, but do not report them. This usually happens for any of three reasons:

1) The risk does not directly impact the person's immediate location, department or budget. This is an example of *silo thinking*.
2) There are sometimes negative personal or career consequences for reporting risks. Some enterprises believe that formal procedures for reporting risks conflict with the organization's risk appetite. Employees then reason that if there are no easy mechanisms or rewards for reporting suspected risks, why do it?**
3) If the process for filtering and escalating risks is not very well developed, the recipient of any reported risk information may be more inclined to bury it than to communicate and manage it.

Any organization that actively encourages its staff to identify and report risks into a structured, formal risk management framework will create a more informed and less vulnerable enterprise.

** *The topic in the second bullet above is central to another book of mine 'Cybersecurity Exposed: The Cyber House Rules'.*

Culture and relationship issues

Many cybersecurity threats are created from within. A corporate culture that creates disaffected or disinterested staff is much more likely to lead to this type of threat than one that fosters employee satisfaction.

In your organization, do people generally like each other, get along nicely and believe that the company invests in them and considers them to be more than assets with id numbers?

When people feel no connection to or support from their organization, they are more likely to seek opportunities to take personal advantage of their position. This is because these individuals often seek to retaliate for the lack of support they receive from the employer.

An organization's whistleblowing process is another factor that reflects the enterprise's culture and also impacts its cybersecurity posture. There are many cybersecurity failures that might have been prevented if company employees and contractors felt comfortable reporting deficiencies through an independent reporting structure that would safeguard their position and anonymity. However, in the real world, the reported issues often end up back with the people that are causing them, together with enough information to identify who reported the problem.

The more open and supportive an organization is toward its people, the more the people will reciprocate. A closed and unsupportive organization will create vulnerabilities through general disinterest from its employees and from rogue insiders who feel justified in using their knowledge and access for personal gain.

It is much easier for a cybersecurity attack to succeed with the help of an insider. An insider does not even need to have privileged access to be capable of providing significant intelligence for a cyber attack. If I have a five minute conversation with a standard employee who is disgruntled, I can usually identify enough security vulnerabilities to identify a cyber attack option. Just imagine what an insider can do if they are motivated.

Never underestimate the extent to which an enterprise's culture correlates with its security posture.

In my own experience, an enterprise with a negative culture will be riddled with security gaps and people ready to help expose them.

Under-investment in security training

Does anybody reading this book maintain a separate username and password for every different web account they use? In a cybersecurity lecture I recently attended at the Royal Institution in London that was packed full of security specialists, about 20% of the hands went into the air.

'325 and counting,' said one person.

Whenever a cybersecurity attack succeeds in obtaining username and password details, one of the first things the criminals are likely to do is to use automated tools to try to re-use the same credentials on all the major web services. But as the cybersecurity lecture statistics reveal, many people, including cybersecurity specialists, are not aware of the importance of using different usernames and passwords for different accounts.

This underscores the greater issue that employees, suppliers and even customers need to be aware of how their actions can create, deter and detect security issues. This fact is deeply relevant to cybersecurity.

When people have access to an organization's digital systems, their actions can affect employees, customers and others as well. This is why anyone with access needs practical and regular awareness training on what the potential security threats are, how to avoid them and how to report any suspected or confirmed security problems.

Security awareness and advice needs to include specific and practical content about security threats to any relevant electronic information or systems to which a person may have access. For example:

- Do not leave your computer or mobile device unlocked when you are not with it and using it.
- Never mix alcohol with using any digital device (phone, tablet or computer) that can access systems at your workplace.
- Never discuss or speak about work when intoxicated.

- Be aware that malicious software can be loaded onto your computer, phone or tablet simply by clicking on a link. For that reason, do not click on any link that you believe may not be safe.

Good security awareness training should be concise, relevant, useful, thought-provoking and frequent. Its content also needs to be updated regularly, meaning at least once per year.

Cybersecurity is not a purely technical problem for the technical team. People are more likely to create cybersecurity failures than technology is. Security awareness is the primary way to make this known.

Using trust instead of procedures

As a species, we tend to use failure as a learning mechanism. Only after something goes wrong do we tend to fix it.

In many organizations, especially in those that are growing, a few select individuals enjoy unbridled privileges and are considered to be completely trustworthy. They have always been there, they have always done the right thing and to add in procedures that move away from the trust system can seem both expensive and unnecessary.

What I have written in the paragraph above is the usual explanation that is used just after an organization was badly burned because trusting an insider proved to be a huge mistake.

Edward Snowden is a great example of this problem. He had worked as a safe pair of hands in government security for years. What could possibly go wrong?

At any point in any process that includes any type of associated privilege, it is essential that procedures are in place to ensure that no one can independently execute an action based on trust alone.

Even if a person is a Chief Information Security Officer (in fact, especially if he or she is), it should not be possible for him or her to directly control and access the security infrastructure he or she is assigned to protect.

The stringency and breadth of procedures that control and monitor access and privilege should always be proportionate to the sensitivity of the assets. The more sensitive the permissions and assets, the greater the need for additional measures to monitor, review, check and approve the actions.

Absence of a single point of accountability

Another cornerstone of security involves ensuring that all aspects of a digital environment that require control and management have a single point of accountability.

> ***single point (of) accountability*** *(SPA or SPOA) – the principle that all critical* **assets***, processes and actions must have clear ownership and traceability to a single person. The rationale is that the absence of a defined, single owner is a frequent cause of process or asset protection failure. Shared ownership is regarded as a significant security gap due to the consistent demonstration that security flaws have an increased probability of persisting when more than one person is accountable.*

Using a single point of accountability has been demonstrated to work incredibly well; it is proved to help control highly regulated systems successfully.

Shared accountability, on the other hand, does not work well. Whenever more than one person assumes ownership and responsibility for certain assets, processes, and actions, the accountability is unclear. In the event of failure, instead of being equally accountable, shared owners expect to be equally unaccountable.

Because of the complex nature of modern organizations, the roles and responsibilities of different owners sometimes overlap, but it's important for decision-makers to prevent this from happening by creating clearly-defined, non-overlapping boundaries.

For example, imagine that I own a system and you own a process that maintains it. Well-defined accountability boundaries would specify that if your process causes my system to break, the resulting defects and the costs and consequences of failure are your responsibility, while the repair of the system and recovery of costs from you are my responsibility.

Social Engineering

One social encounter can compromise the best cybersecurity in the world. Social engineering (traditional espionage and more) is the most fascinating of the human factors.

> ***social engineering**** *– is the art of manipulating people through personal interaction to gain* ***unauthorized access*** *to something.*

It constantly surprises me that it is so much easier to steal information by exploiting social situations than through direct attack.

If you put on a boiler suit with a logo, carry a clipboard and have a sense of confidence, you can physically access a lot of sites that you should not be able to access. However, most social engineering that can impact cybersecurity is far less risky.

An attack team that blends espionage and geek is very effective. Unfortunately, it is very easy for such a team to intentionally place agents in situations in which they can get close enough to 'trusted' people, or can worm their way inside trusted suppliers premises or systems to extract very sensitive information.

Whenever anyone develops a friendship with someone else, he or she will have a propensity to disclose and discuss information – including information about the workplace. A small amount of insider knowledge divulged during such conversations, even from a non-technical person, can easily give a surreptitious attacker enough ammunition to bypass many layers of security.

The main protection against social engineering is through awareness training, with real life examples. Here is an example:

Bob worked as the only security guard in the main lobby of a building with 1,000 employees. The access control gate was too slow to operate in the mornings, so instead, Bob had to individually buzz the gate open for each employee. Security had become relaxed, and people were used to greeting Bob with a ‘Hey Bob,’ followed by Bob buzzing them in. It was clear from the look on Bob’s face that he probably had no idea who most of them were. Perhaps he knew a few hundred of them.

Here are my social engineering questions:

- If I told you this story in a bar and divulged where I worked, do you think you could get into my building?
- If you visited the lobby once for a legitimate reason, do you think you might have noticed this security gap?

Many cybersecurity attacks are crimes of opportunity. Social engineering attacks are also not always premeditated. If the wrong information is passed to the wrong person at the wrong time, the opportunity can facilitate the attack.

As part of any defense-in-depth strategy, it is essential to consider that human factors are the most likely to create the opportunities that lead to a cybersecurity failure.

If you are a cybersecurity professional and ever get the chance, add a question on human factors to the root cause analysis section of any incident response procedure. Something like this:

Were any of the following human factors identified as contributing toward the security failure?

- Gaps in the procedures that should have been in place.
- Risks that were known to some but not reported or managed effectively.
- Disinterested or disaffected personnel.
- A lack of security awareness by any of the people involved.
- A level of access privilege that was not adequately monitored or segregated.

- Any form of social manipulation or fiction by an individual to gain access to information or systems.

There are, of course, another set of human factors to consider – the profile and philosophy of the people who instigate cyber attacks. These factors are considered in Chapter 11: The Cybersecurity Cold War.

Before we discuss who initiates and perpetrates cyber attacks, we need to complete our understanding of cyber defense. To do that, we now need to cover the central core of cyber defense.