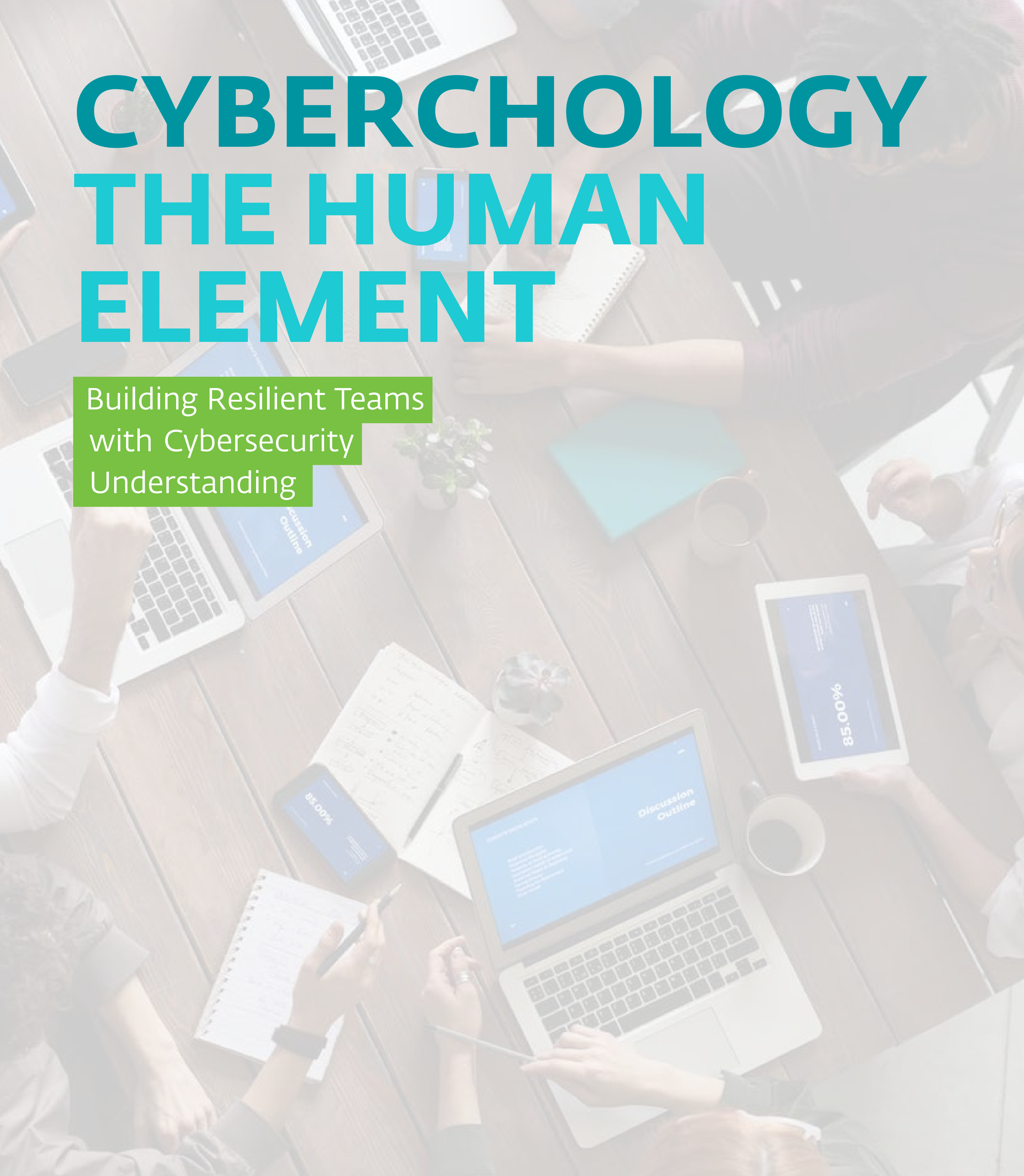
ENJOY SAFER TECHNOLOGY™

The Myers-Briggs Company

CYBERCHOLOGY THE HUMAN ELEMENT

Building Resilient Teams with Cybersecurity Understanding



Cybersecurity has become the most important consideration for any modern business. A majority of organisations inhabit the online world in some shape or form, and technology is at the core of most business functions. With the COVID-19 pandemic acting as a catalyst for accelerated digitalisation across almost every industry, the pressure to be resilient and dynamic in the face of change has heightened.

For this Cyberchology paper, ESET, a global leader in IT security, has partnered with leading business psychology organisation The Myers-Briggs Company to explore the critical role employees play in keeping organisations safe from online threats, investigating the link between personality type and vulnerabilities to cybercrime. The paper also examines the attitudes and experiences of over 100 Chief Information Security Officers on cybersecurity during the COVID-19 lockdown.

Since the British Government implemented the COVID-19 lockdown in March, the world of work has changed dramatically in ways most people could not have envisioned. The result – mass implementation of remote working that has seen a heavier reliance on technology than ever before, and a resultant disruption of many businesses' technology infrastructures. Central IT systems have been substituted with a network of disparate individuals, all with a greater responsibility for their own technology use and cybersecurity needs. Not only does a fractured security system leave companies vulnerable, but employees' confidence in handling cybersecurity is also a serious risk.

The cybersecurity landscape is constantly evolving to mitigate the increasing sophistication of cyberattacks, and COVID-19 has only exacerbated this. ESET's research found that since lockdown began, cybercrime has increased by 63%, and businesses are right in the firing line due to their now dispersed workforces. As we will explore in this paper, remote working is here to stay, and businesses must adapt their cybersecurity strategies accordingly. An organisation's cybersecurity rests in the hands of every employee with fingers on a keyboard and cannot be a business issue for IT teams or senior leaders alone.

At a time when businesses are relying on resilience, malicious actors are exploiting the security vulnerabilities that accompany remote working. Simple measures such as using a virtual desktop interface or requiring encryption for sensitive files can reduce the likelihood of a successful attack. ESET's research for this report revealed that more than half of businesses did not have continuity measures in place for a potential pandemic before the COVID-19 outbreak, and while 80% said they did have a remote working strategy in place, only a quarter of businesses would consider their remote working strategy and operations plan effective.

If businesses are to thrive rather than just survive, a holistic cybersecurity strategy that takes individual personalities into account alongside a comprehensive endpoint software solution is crucial. With so much responsibility resting on employees all working from different locations, devices and networks, a self-awareness of positive cybersecurity habits and personalised cybersecurity training is essential. This paper will explore why and how HR and Tech teams should work together to build resilient IT systems, strategies and teams, for a resilient business.

Cybersecurity challenges

Prior to COVID-19, cyberattacks were already on the increase, and the pandemic and resulting lockdown has only heightened this risk. From phishing scams to COVID-19 related malware, cybercriminals have pounced on the innate vulnerabilities of dispersed workforces and their IT systems. CISOs reported a 63% increase in cybercrime during lockdown – all while many businesses have been struggling to stay afloat or rapidly adapting their business and operational models to survive. The pandemic has changed the world of work as we know it, and businesses will need to adapt their cybersecurity strategies to reflect this.

In addition to the operational and reputational costs of an attack itself, the fines issued by regulatory bodies are increasing. Prior to the pandemic, the Information Commissioner's Office (ICO) issued two multimillion-pound fines against British Airways and Marriott, under the General Data Protection Regulation (GDPR) rules. Although huge corporations have the deep pockets to deal with the ramifications of an attack, smaller businesses may well be crippled.

ESET's research revealed that for 75% of companies, half of their business is being undertaken by employees who are working remotely that were not doing so before COVID-19. Conversely, less than 25% of businesses said they were unable to work because they could not carry out their projects remotely. Although employees will eventually return to the office, remote working in some form is here to stay. Many businesses have been able to operate remotely during lockdown, albeit with adapted systems and processes. Though the transition was sudden, businesses were forced to innovate, illustrating that it is in fact possible to do much of our work from afar.

Remote working has brought flexibility, but it has also dramatically altered business processes and systems in order to cater to a distributed workforce. Employee access to IT departments, and vice versa, has changed. Collaboration and teamwork is facilitated virtually, and a lack of face-to-face communication can hinder direct channels of communication. Some of the baseline security measures taken for granted in the office must be compensated for at home, such as requiring home workers to use multi-factor authentication or a VPN to access internal networks. Reminding workers to enable automatic updates and check the security of their own Wi-Fi networks is also crucial as the first line of defence against cybercriminals.

When evaluating the challenges associated with employees who are working from home, 80% of companies said that an increased cybersecurity risk caused by human factors posed some sort of challenge. In addition, 37% of companies said workplace digitalisation and the shift to online processing has been challenging. With the combination of fractured business IT systems and a lack of central security, a sudden shift to remote working and a global climate of stress and concern is the perfect breeding ground for a successful cyberattack.

Key challenges reported by businesses during the COVID-19 lockdown

80%
increased cybersecurity risk caused by a human factor

51%
identity authentication

63%
cybercrime increase

46%
the need for short-term investment

53%
integration of solutions

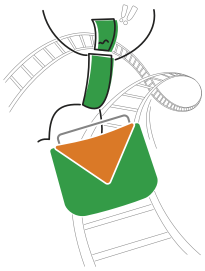
37%
workplace digitalisation and the shift to online processing

The impact of stress on cybersecurity habits

The coronavirus crisis has added an extra layer of stress and concern to our everyday lives. It can be hard to concentrate and remain motivated at work, leaving employees more vulnerable to cyber threats. In the report **'Personality and stress in a virtual world'**, The Myers-Briggs Company found that 47% of respondents were somewhat or very concerned about their ability to manage stress during the coronavirus crisis, with the economy going into a recession and the health of family and friends as key concerns. This persistent undercurrent of stress affects different personality types in different ways, and manifests in the ways different people manage stress and respond to certain situations. Already stressed employees may be more likely to panic and click on a malicious link, or a lack of attention to detail may result in a security breach not being properly reported to IT.

Knowing more about your MBTI type can help. Here are some things that stress out each type, according to the most well-used part of their personality – their Core Character™, and how each type tends to behave when under pressure.

Activist (ESTP & ESFP)



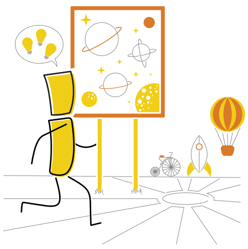
Stressors

- Lack of stimulation and excitement
- Theoretical, abstract tasks without practical application right now
- Being physically confined, e.g. through illness or circumstances

Behaviour under everyday stress

- Seeks more and more external stimulation and excitement
- May behave in a thrill-seeking or dangerous way or over-indulge
- Lives solely in the present moment and will not make any decisions

Explorer (ENTP & ENFP)



Stressors

- People who say "it'll never work"
- Too much seemingly irrelevant detail
- Lack of variety; not being able to do anything new

Behaviour under everyday stress

- Shares increasingly impractical ideas with more and more people
- Unable to take things seriously, becomes destructively 'playful'
- Will not be tied down to decisions

Director (ESTJ & ENTJ)

Stressors

- Inefficient people, systems, or organisations
- Lack of closure, not being able to make decisions, blockers
- Having to focus on people's feelings, rather than the task

Behaviour under everyday stress

- Becomes overly directive, forceful, even aggressive
- Makes snap decisions and imposes them on others
- Dismisses evidence/other opinions that do not fit their view

Nurturer (ESFJ & ENFJ)

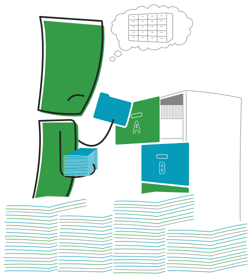
Stressors

- Conflict with others and between others
- Lack of warmth, not having their friendliness reciprocated
- Injustice in the world at large

Behaviour under everyday stress

- Becomes effusive and over-friendly
- Demanding in getting their own and others' needs met
- Interprets situations in terms of their values, ignoring any evidence

Conserver (ISTJ & ISFJ)



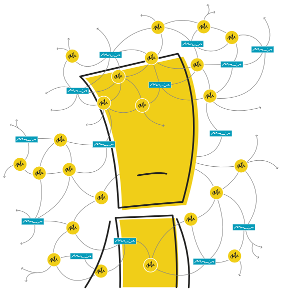
Stressors

- Having to act without detailed, practical information or plans
- Others who dismiss the lessons of the conserver's past experience
- Changing things that already work

Behaviour under everyday stress

- Obsessively searches for that one important piece of information
- Withdraws from the outer world
- Cannot make a decision until all the information has been found

Visionary (INTJ & INFJ)



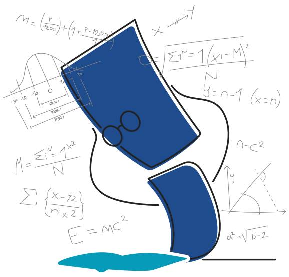
Stressors

- Not having time to think through possibilities before answering
- Having their well-considered ideas dismissed or ignored
- Disorganised, opinionated people

Behaviour under everyday stress

- Withdraws, to build increasingly complex ideas in their head
- These models may become divorced from reality
- Unable to act until every possibility has been explored

Analyst (INTP & ISTP)



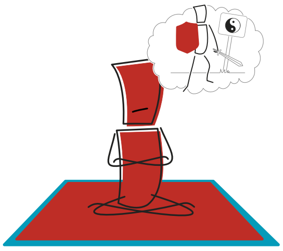
Stressors

- Having their carefully reasoned solutions dismissed or ignored
- Illogical decisions that have not been thought through
- Excessive displays of approval or emotion from others

Behaviour under everyday stress

- Withdraws to solve problems by themselves
- Fixates on finding the one correct solution
- Ignores other people; makes decisions without informing them

Conscience (ISFP & INFP)



Stressors

- People who ignore, dismiss, or contravene their values
- Working in a job that is at odds with those values
- Inflexible and unthinking people or organisations

Behaviour under everyday stress

- Withdraws into an inner dialogue
- Obsessively works through decisions that fit with their values
- Ignores facts that do not fit with the picture they have painted

Resilience

As we grapple with a paradigm shift in our work and home lives, resilience is more important than ever. With over 50% of businesses planning on keeping the changes made during COVID-19 in place in some shape or form, how organisations can build resilience into their IT systems and teams must be top of mind.

Confident employees who are educated on cybersecurity best practice are the foundation of a resilient strategy. As ESET discovered from its Catphishing research, which looked at the cybersecurity habits of 2,000 employees in the UK, 69% of Brits say they are concerned about their cybersecurity but have no clue what to do about it, with 68% of 25-54 year olds and 55% of over 55s admitting to having concerns or worries about cybersecurity. Although employees in the 16-24 age bracket worried less, this does not necessarily mean that they would be less likely to fall victim to an attack as complacency, a lack of skills, and shortfalls in training can leave businesses vulnerable.

> **“ESET's Catphishing research, which looked at the cybersecurity habits of 2,000 employees in the UK, discovered that 69% of Brits are concerned about their cybersecurity but have no clue what to do about it, with 68% of 25-54 year olds and 55% of over 55s admitting to having concerns or worries about cybersecurity.”**

Despite a clear increase in cybersecurity threats and a lack of employee skills, 40% of CISOs reported that COVID-19 had no impact on the size of their IT security budget, compared with the original planned budget. This oversight may leave businesses exposed to future cyberattacks, and without the adequate resources to mitigate. IT teams are having to rethink the way organisational security operates as remote working becomes the norm, not the exception.

The overwhelming majority of cyberattacks are successful not because of the hacker's skill, but due to human error or oversight. In fact, 80% of companies reported that a significant challenge during COVID-19 was the increase in cybersecurity risk caused by the human factor. The ways in which people prefer to digest information and communicate can play a role in how different team members approach cybersecurity, as all personality types have different strengths and blind spots that can impact the outcome of a cybersecurity attack.

The Myers-Briggs Type Indicator (MBTI) personality model looks at four areas of personality type – Extraversion or Introversion, Sensing or Intuition, Thinking or Feeling and Judging or Perceiving – and how these areas combine dynamically to describe the whole person. For example, those with more Extraverted personality types (those who work out ideas by talking them through) tend to be more vulnerable to manipulation, deceit and persuasion from cybercriminals, while those with a preference for Sensing (those who observe and remember details) are more likely to spot phishing attacks, and also more likely to take cybersecurity risks. While different personality preferences do not guarantee cybersecurity awareness or knowledge, building self-awareness and an understanding of personality into cybersecurity training is a starting point in understanding where cybersecurity weaknesses may lie.

If human error is responsible for a majority of cyberattacks, then businesses cannot ignore the impact of human traits and characteristics on employee cybersecurity habits. Cybersecurity has long been thought of as the responsibility of IT departments alone, but to build a holistic cybersecurity strategy that accounts for the human factor, IT and HR departments must work together. Using psychometric testing and self-awareness tools, HR can help to identify the make-up of teams and pinpoint where potential vulnerabilities exist. IT teams can use this insight to create comprehensive security protocols and a proactive cyber strategy to stay one step ahead of potential threats.

Accounting for personality preferences can make cybersecurity training more engaging and effective too – by delivering broader training at induction and following it up with regular check-ins and updates that are tailored to employees' personalities, good cyber hygiene and security habits are more likely to be adhered to. This is particularly important considering the move to mass remote working by many businesses. As IT teams have less visibility and physical access to individual employees, ensuring your workforce is properly educated on cybersecurity best practice is vital in protecting the entire organisation.

The cybersecurity landscape has evolved significantly in the past 12 months, as some threats have disguised themselves and resurfaced in various forms. At their core, most of these threats can be identified as malware or phishing; malicious attacks on organisations' systems can be avoided when people understand themselves and are self-aware about what type of attack they might be vulnerable to. In doing so, organisations can be proactive in mitigating cyber risks.

Common trends

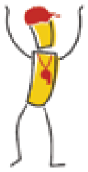
Phishing

Commonly carried out by email, phishing is an online scam where the cybercriminal impersonates a trustworthy entity in order to obtain the victim's sensitive data.

The Sednit group – also known as APT28, Fancy Bear, Sofacy or STRONTIUM – has been operating since at least 2004 and has made headlines frequently in recent years. On August 20th, 2019, a new campaign was launched by the group targeting their usual victims – embassies and Ministries of Foreign Affairs in Eastern European and Central Asian countries. The latest campaign started with a phishing email containing a malicious attachment that launches a long chain of downloaders, ending with a backdoor.

Personality types such as ENFP and ENTP may find themselves vulnerable to phishing-related attacks such as those used by the Sednit group that use a simple email format. While both ENFPs and ENTPs can be IT-savvy, the best practice for these personality types will include taking their time to check the validity of the emails they receive before responding, and being suspicious of emails with intriguing content or an emotional appeal.

ENFP



- ENFPs are one of the first to realise when a new security process is in place
- Will take IT security very seriously if it becomes one of their values

Cybersecurity tips:

- Be suspicious of emails that have an emotional appeal for you
- Stop and think before you click

ENTP

- IT-savvy ENTPs will strive to be competent and avoid 'stupid' errors
- Keen to make things happen (though this can mean bending the rules)

Cybersecurity tips:

- If you compromise security, others may see you as incompetent
- Slow down before you read emails – you might spot something

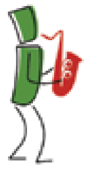
ESTP

- When they are persuaded that cybersecurity is important, ESTPs can quickly spot when things are not right and take immediate action

Cybersecurity tips:

- IT security is important, and the rules do apply to you
- Get specific examples of what you can do differently, and act on them

ESFP



- ESFPs will take quick action when they spot that something is not right
- Generally, they follow IT security rules and policies

Cybersecurity tips:

- Don't trust a public network for sensitive data even if it has a password
- Don't take things for granted – it pays to be vigilant, perhaps even untrusting

ISTJ

- ISTJs are likely to spot discrepancies and errors in phishing emails
- Generally, they follow IT security rules and policies

Cybersecurity tips:

- Don't just use variations on the same password or passwords
- Stay alert. Previous experience should not be your only guide

ISFJ

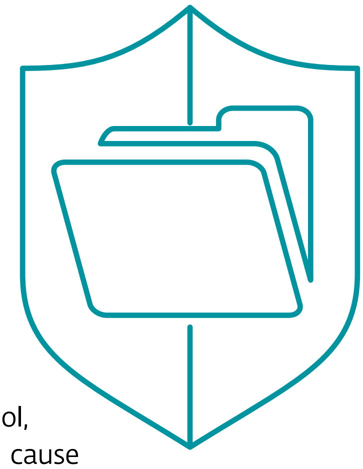
- ISFJs are likely to spot discrepancies and errors in phishing emails
- Unlikely to be caught out twice by the same cyberattack

Cybersecurity tips:

- Don't trust a public network for sensitive data even if it has a password
- Be careful who you trust. Online, people may not be who you think

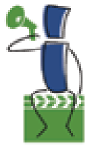
Malware

Malware comes in a wide variety of forms, including viruses, spyware, and ransomware – all of which can compromise your computer and data. DePriMon is a recent example of a malicious downloader, with several stages of infection and using many non-traditional techniques. To achieve success, the malware registers a new local port monitor – a trick falling under the "Port Monitors" technique in the MITRE ATT&CK knowledgebase. For that, the malware uses the "Windows Default Print Monitor" name; disguising its malicious nature.



Personality types such as ESTJ and ENTJ may be more vulnerable to malicious downloads that are disguised as legitimate software or modules. While they are usually ahead of the curve on security protocol, this tendency could cause them to make a quick decision for the sake of efficiency. These personality types should focus on taking in all relevant information before making decisions, and ensuring they consult those with a broader knowledge of IT security.

ESTJ



- ESTJs are likely to follow IT security rules and processes and seek to improve them
- Generally, they take cybersecurity seriously

Cybersecurity tips:

- Don't always do things the same way or use the same passwords
- Don't be tempted to cut corners in order to be more efficient

ENTJ

- ENTJs are one of the first types to realise when a new security process is in place
- Will keep up to date and ask questions to understand security issues

Cybersecurity tips:

- Don't rush to change security processes – find out more first
- Avoid overruling others if they have a fuller knowledge of IT security

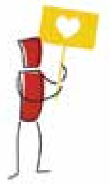
ESFJ

- ESFJs are aware of IT security policies and follow them conscientiously
- They form security habits and use them to follow the rules efficiently

Cybersecurity tips:

- Be careful who you trust. People online may not be who they seem
- Don't always do things in the same way, or use the same passwords

ENFJ

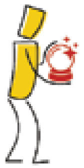


- Will follow the rules when the rules are clear
- Will take security seriously when aware of effects of breaches on people

Cybersecurity tips:

- Be proactive about IT security, even at home
- Don't re-use passwords or use the same one for different apps

INFJ



- INFJs can over-complicate things and search for hidden meanings. This can be an asset in IT security

Cybersecurity tips:

- If something doesn't feel right then check, check and check again
- Don't forget to check details – they are important!

INTJ

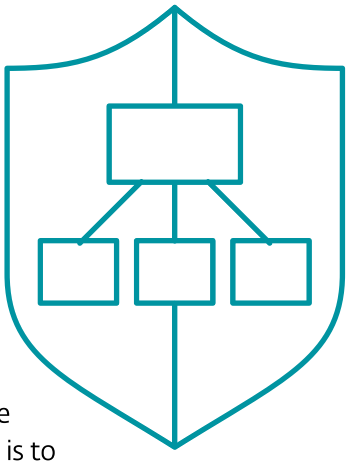
- INTJs value knowledge and strive to be capable and competent
- Generally, they follow IT security rules and policies

Cybersecurity tips:

- You don't necessarily know best, even if the rules seem unnecessary
- If you want to be competent, remember to check the details of emails

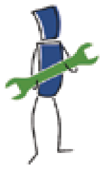
IoT

Our lives have become increasingly overrun with devices, often all connected to each other and running off the same networks and connected systems. Whether at home or at work, our connected devices create vulnerabilities for entire systems if each device is not properly secured, such as a personal phone or smartwatch that may be connected to a work network. Recently researchers found that for one smartwatch model, they were able to access the location, phone number, photos and conversations of well over 5,000 children, due to the manufacturer not securing their servers properly.



Personality types such as ISTP and INTP may find themselves vulnerable when taking matters into their own hands regarding connected devices, even if they are normally rule followers. The best practice for these personality types is to not always assume that you know best, and to make sure you're not ignoring rules or protocols because you think they may not apply to you.

ISTP

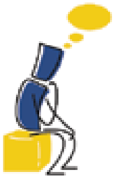


- ISTPs have a healthy mistrust of systems and of other people online
- Happy to follow IT security rules when they make logical sense

Cybersecurity tips:

- Make the effort to find the reasons for a rule before you bend it
- Doing things in your own way quickly in the moment can be risky

INTP

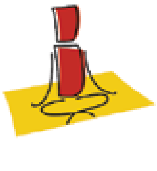


- Many INTPs are knowledgeable about cybersecurity issues
- INTPs are very aware that anyone can be caught out by cyberattacks

Cybersecurity tips:

- Find the IT security rules for your organisation and follow them
- You don't always know best! The rules are there for a reason

INFP

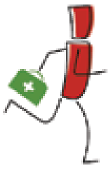


- INFPs are unlikely to make sudden, risky choices
- If aware of the effects of poor security on others, they can see the need for rules

Cybersecurity tips:

- Your organisation will have IT security rules. Follow them
- To avoid harming others, take personal responsibility for IT security

ISFP



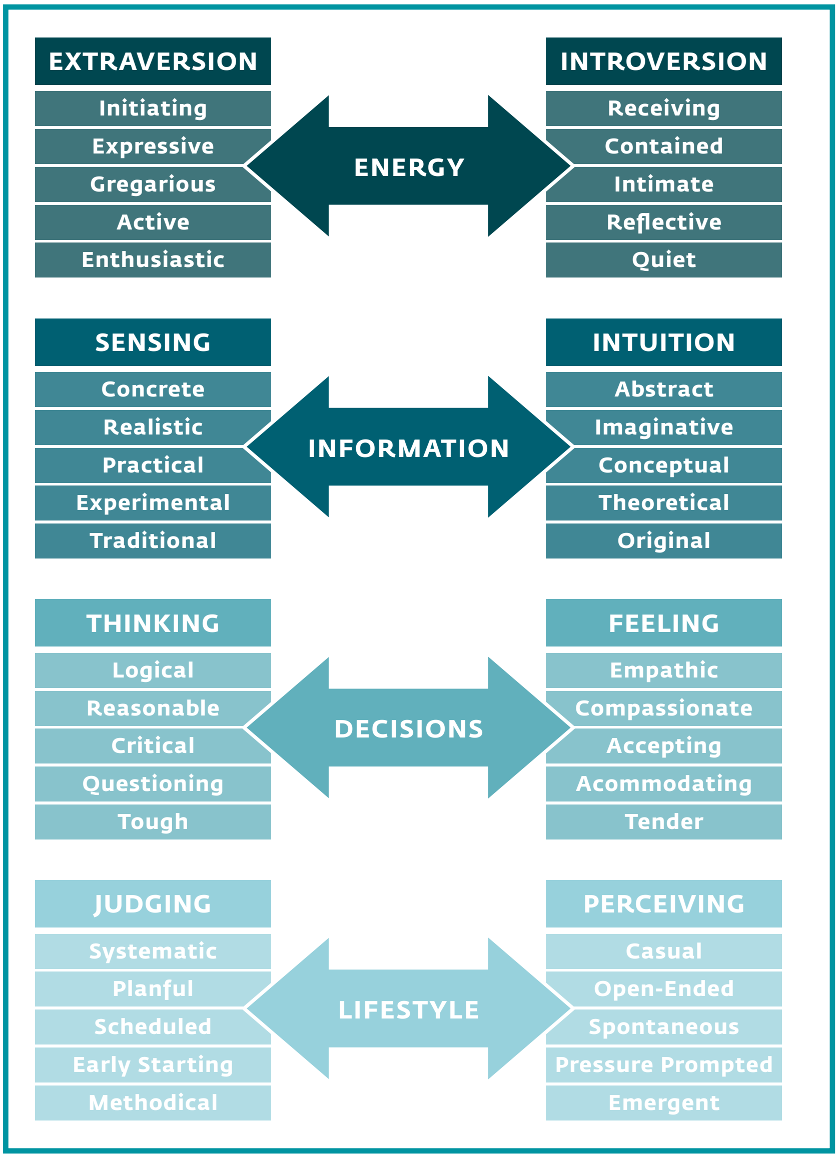
- ISFPs take IT security seriously and are careful in their online behaviour
- Generally, they follow IT security rules and policies

Cybersecurity tips:

- Pause before you click
- Remember that people online, even friends, may not be who or what they seem

Leadership

Strong leadership is at the core of a resilient business. Just as a physically dispersed workforce has impacted the nature of cybersecurity, so too has it influenced the way we view effective leadership. We look to leaders in times of crisis for motivation and reassurance, and the ability of a leader to instil an authentic concern and awareness around cybersecurity is an essential part of keeping businesses safe. Cybersecurity is a company-wide issue, not one for senior leaders to tackle or dictate alone.



EXTRAVERSION	ENERGY	INTROVERSION
Initiating		Receiving
Expressive		Contained
Gregarious		Intimate
Active		Reflective
Enthusiastic		Quiet
SENSING	**INFORMATION**	**INTUITION**
Concrete		Abstract
Realistic		Imaginative
Practical		Conceptual
Experimental		Theoretical
Traditional		Original
THINKING	**DECISIONS**	**FEELING**
Logical		Empathic
Reasonable		Compassionate
Critical		Accepting
Questioning		Acommodating
Tough		Tender
JUDGING	**LIFESTYLE**	**PERCEIVING**
Systematic		Casual
Planful		Open-Ended
Scheduled		Spontaneous
Early Starting		Pressure Prompted
Methodical		Emergent

Much like the weakest link in a chain, an employee at any level of seniority is capable of putting a business in danger, so a traditional top-down approach to leadership is not necessarily the way to harness support for cybersecurity awareness. In addition, senior business leaders are often subjected to attacks at a higher rate, such as spear phishing – the practice of a targeted malware attack, often using personalised information in order to appear legitimate. Whether you will fall victim to a cyberattack has little to do with seniority, and far more to do with education and awareness. For a cybersecurity strategy to function effectively, it is imperative that positive cyber habits and processes are instilled in the culture of organisations and are not seen as a chore or burden.

Earlier in this paper, we recommended 'type tips' for different personalities regarding both stress and cybersecurity. While these tips are certainly a good starting point for identifying individual strengths and weaknesses, it is important that businesses take into account how different personality preferences manifest in a team dynamic. The way a team interacts has a direct effect on how they respond to a cyberattack and the elements of cyber hygiene that might fall by the wayside in moments of stress or panic. Leaders must also recognise their own personal strengths and weaknesses to encourage self-awareness within the team and wider organisation.

By building their own self-awareness, leaders can not only understand themselves better but begin to appreciate the nuances of behaviour amongst their team, their department and their organisation. The MBTI type framework is an effective and straightforward way to do this, but leaders who want to deepen their understanding further often find the MBTI Step II assessment useful. For each of the four MBTI preferences, Step II looks at five facets of behaviour, giving a personalised picture of the individual. For example, most people with a preference for Extraversion will feel comfortable initiating conversations with strangers in social situations (Initiating), but some will prefer to take a back seat and wait for others to come to them (Receiving). Conversely, most people with a preference for Introversion will take the Receiving role, but others will show Initiating behaviours. Step II feedback can be especially useful for leaders who find they are misunderstood by their staff.

Team self-awareness is just as important as individual self-awareness when it comes to cybersecurity. Understanding the Step II profile of a team can help to identify the gaps in behaviour where a cyberattack could slip through and can help HR and IT teams to deliver personalised cybersecurity training based on team needs.

Conclusion

Regardless of what the future will bring, two things are certain – the way we work has been permanently altered and cyberattacks are not going away. The COVID-19 pandemic has only accelerated the implementation of technology across all facets of life, and as more and more of our working and home lives become digitised, cybersecurity will remain the lynchpin of business safety. Cyberattacks are a persistent threat to organisations, and businesses must build resilient teams and IT systems to avoid the financial and reputational consequences of such an attack. An understanding of personality can play a key part in any business's cybersecurity strategy, both enhancing the effectiveness of training and encouraging employees to be more invested in their own self-awareness and skills. Understanding that the human element of cybersecurity is just as important as the technical is the first step in building holistic protocols that account for individual strengths and blind spots.

In times of crisis, leadership has a profound impact on organisational culture and morale. When leaders are self-aware and aware of their teams, they can instil processes and practices more effectively and guide other employees in their own self-awareness journey. Strong cybersecurity practices must be engrained across all levels of an organisation and investing in employee training, both in cybersecurity and self-awareness, will allow IT and HR teams to build integrated, effective and proactive cybersecurity strategies.