WORLD FEDERATION OF EXCHANGES

Cyber Security for Exchanges & Post-Trade Infrastructure

Staff Behaviour and Culture

Introduction

The World Federation of Exchanges (WFE)[1] and its members who operate exchanges and CCPs (collectively "WFE members") are highly incentivised to ensuring the trading and clearing environments they operate are secure, stable and resilient. This is fundamental to their business.

Exchanges and CCPs spend significant time and money on ensuring the technology that underpins the markets they operate and clear meet – and exceed – the complicated patchwork of technical standards, rules and regulations they are subject to.

However, they are reliant not only on technological defences, but also the humans that work within and operate that technology. The WFE hereafter provides the thoughts of the global exchange and CCP industry on best practice for staff training and cyber awareness in order to make more secure the technology defences they also deploy.

This is in the dual interests of:

- Acting as a reference point for future dialogue with regulatory authorities as they continue to consider how best to strengthen the system in response to an ever-increasing degree of sophistication of cyber-criminals; and

- Providing a common set of industry best practices to be considered when designing staff training and awareness programmes, and in order to benchmark arrangements against.

Background

WFE members continue to prioritise cyber resilience to ensure the strength of their markets, particularly given the level of interconnectedness amongst themselves and other financial market participants. Indeed, exchanges and CCPs are now essentially technology driven companies that offer trading and clearing facilities for the wider market. As a result, they invest in significant levels of highly qualified technology staff. At the same time, they are highly motivated (for commercial, reputational, financial stability and regulatory reasons) to ensure their systems, and the wider financial system in which they operate, are robust, resilient, stable and regularly tested.

Markets are global, and the financial system is highly interconnected. However, risk tolerance, threat landscape and systemic nature vary from market to market; each operates in different legal and regulatory environments, are at different stages of maturity, and apportion differing cyber budgets. What is common, however, is the seriousness with which WFE members take their technology security obligations. They invest significant time, money and human resource into designing systems and technological defences that are best-of-breed and can stay one step ahead of attackers.

Nevertheless, it is also the case that the system is only as strong as its weakest link. Evidence shows that, often, the weakest link is not the technology, but the human beings operating within companies. It is often quoted that more than 90% of all cyber security incidents involve some form of human error[2]. Building the human firewall is therefore a key strategy all exchanges and CCPs should promote.

[1] WFE is the global industry association for exchanges and clearing houses. It represents more than 200 market infrastructure providers, of which more than 100 are Central Counterparties (CCPs) and Securities Depositories (CSDs). Its members include exchange groups and standalone CCPs.
[2] IBM X-Force Threat Intelligence Index

As a result, firms are increasingly looking towards how to most effectively engender a culture of cyber compliance, moving away from classroom based, infrequent refresher sessions (which can be seen as an inconvenience in staff's otherwise busy diaries), and thinking more creatively around how to get staff buy-in and consideration of cyber defences in everything they do. Exchanges and CCPs are no different.

Nudge Theory & Behavioural Economics

Nobel Economics laureate Dr Richard Thaler[3] describes how humans do not take decisions based upon a rational basis. Instead economic decisions tend to be based on personal biases, emotion and the environment they are in. This also holds true for the subject of cyber security. It is observed that at work we don't always do the things that might improve our organisation's security, and at home we sometimes take shortcuts that leave us vulnerable.

Some[4] believe that behavioural insight models rely to a greater or lesser extent on a number of principles, which may include:

- Rational choice-based models assume that people will interpret all information available to them, then behave in a way that will result in the greatest benefits;

- Models of planned behaviour assume that if a person intends to act in a certain way then they will. Intention to behave is influenced by attitudes towards that behaviour;

- Protection motivation models believe that people's behaviour is influenced by their perception of threats and perceived ability to cope, which interact and influence behaviour;

- Learning models assume that behaviour is a learned process and learning is influenced by both incentives (rewards and punishment) and our social environment (e.g. role models); and

- Change models assume behaviour change is a process, with various stages and not a single event.

Indeed, many companies are finding that applying behavioural insights and 'nudge theory' can be useful to change staff security behaviours. By applying small nudges frequently to staff, they are encouraged to talk about cyber, and far better cultural outcomes are often observed. Examples of this include introducing fake phishing scams, educating staff who click on them, rewarding those who avoid/spot attacks, and taking further action on those who persistently do not.

This theory that a small incentive, or nudge, can change behaviour is increasingly being taken on board by both public[5] and private[6] organisations with some evident success, proving even small incentives can help change and maintain good behaviour. Popular examples of nudge theory at work can be found below[7].

Security nudging and behavioural insights are however only one tool for encouraging good security behaviour, and should sit alongside efforts to challenge beliefs and underlying assumptions. These assumptions are key to changing security behaviours, such as an individual believing they won't get phished, or not stepping in to stop that person they don't recognise.

As one tool in the box, this can be simple and cheap, and are proven to have big fast acting impacts when they effectively tap into the decision environment.

The below guidelines set out best practice examples for engendering a staff culture of cyber security compliance. This is a non-exhaustive list compiled by the WFE's dedicated cyber security group of more than 30 information security professionals within global exchange and CCP groups, drawing upon their collective experience of what works well and what has proven to be less effective in approaching staff training and behaviour around cyber security.

[3] "Nudge" – Dr Richard Thaler and Cass Sunstein - 2008

[4] The Government Office for Science, or GO-Science

[5] Such as the UK Tax Authorities – HMRC – who have seen increased tax revenues

[6] Including a range of US pensions suppliers – who have encouraged more people to save for the future after automatic enrolment in pension plans, and a Swiss corporate security team, who rewarded those staff following the 'clear desk' policy with a small chocolate - rather than highlighting the cluttered desks with large yellow reminder notes.

[7] Cyber Security: A Nudge in the Right Direction

WFE Best Practice Guidelines

Engendering a Staff Culture of Cyber Security Compliance

Whilst acknowledging the need for flexibility and to design staff awareness and training programmes targeted to the specificities of individual companies and cultures, below we provide examples and best practice guidelines for WFE members to consider as the building blocks on which their individual approach could be based.

Behavioural Incentives

- Focus on the home environment - staff are more likely to be cautious if they see the risks of breach on their personal network than work;
- Bringing into the workplace hackers to demonstrate to staff how easily devices can be compromised, particularly via Wi-Fi;
- Linking compensation to compliance – for example reducing bonus payments for repeated testing failures, or contractual obligations / fines;
- Rewards programmes for identifying potential breaches or suggesting a strengthening of approach;
- Awareness campaigns noting how frequently others are making referrals – so called “bandwagon effect”; and
- The use of “Gamification” – specifically making desired security behaviours fun or competitive.

Cultural Incentives

- Create a culture of personal responsibility and common sense – relate cyber awareness to personal life, family and home as employees tend to take cyber awareness more seriously when it has a personal message;
- Make cyber security awareness and compliance a Key Performance Indicator / staff objective to highlight its importance;
- Cyber messaging will be more memorable if the language around security issues is simple, jargon-free, creative and graphical; and
- Story telling – creative use of language using analogies and anecdotes to create mental imagery and explain complicated concepts.

Operational Support to Engender Staff Awareness and a Compliance Culture

Training

- Ensure there is regular and “accessible” cyber security staff awareness training;
- Ensure there is specific compliance and education / cyber security training for new joiners;
- Avoid the mistake of not training technical staff on cyber awareness – they are often the first target in cyber attacks;
- Create a sense of ownership of compliance through deployment of a strong password policy and requiring the locking of computer screens when away from the desk;

Transparency

- Ensure robust security policies are planned and implemented, and are clear and available to all;
- Enforce security policies and measure compliance levels across the board;
- Share your disaster recovery and post-breach communications plans with employees, and be open to their suggestions and observations;
- Provide a list of approved websites, services, software and applications – and those that are restricted;

Technology

- Asking employees who use their own devices at work to install anti-virus software and to switch on firewalls / develop an electronic device usage policy (including “bring your own device” or “BYOD” guidelines); and
- Deploy software tools that launch phishing emails against your employees but operate under your control – in order to test whether employees are likely to fall prey to a phishing attack.

Annex

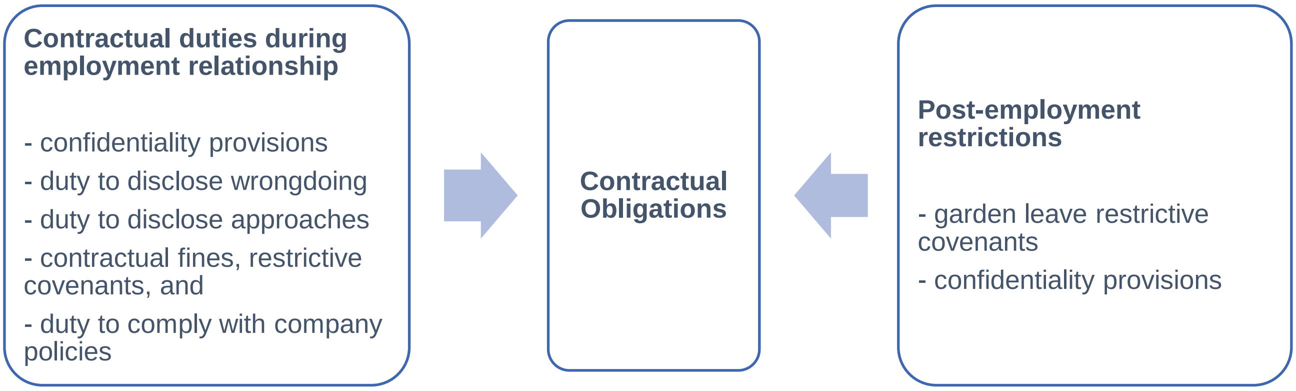
Examples of Notable Behavioural Insights

Allen & Overy

Allen & Overy released a white paper in 2016 on whether cyber-attacks in the workplace was an employment issue. Several human elements are highlighted as the biggest risks to employers. In general, employees who cause security breaches either do so negligently, i.e. human error (Type A), or they facilitate a data breach deliberately (Type B). Negligent behaviour can include an employee using a personal USB-stick in the office and inadvertently introducing malicious software, or opening a malicious email/attachment. Reasons behind the actions of Type B employees can include, (i) espionage for national security agencies, (ii) acting on behalf of a competitor, or (iii) own monetary/emotional interest.

It is important for organisations to undertake certain preventative as well as disciplinary measures to minimise the risk, these include:

- **Pre-employment vetting**: vetting is recommended to detect Type B employees.
- **Employment monitoring**: monitoring internet and email use of employees is an effective action in preventing cyber-attacks. However, strict data protection regulations apply.
- **Education and training**: regular and consistent training and education of cyber security protocols.
- **Contractual protection**: experience suggests that employers are currently not using the employment contract effectively to mitigate cyber security risks. There are two types of contractual obligations, (i) those dealing with the duties of employees during the employment relationship, and (ii) post-employment restrictions.



Contractual duties during employment relationship

- confidentiality provisions
- duty to disclose wrongdoing
- duty to disclose approaches
- contractual fines, restrictive covenants, and
- duty to comply with company policies

Contractual Obligations

Post-employment restrictions

- garden leave restrictive covenants
- confidentiality provisions

Behavioural Insights Team

The Behavioural Insights Team, set up by the UK Government and now co-run by them, say that "if you want to encourage a behaviour, make it Easy, Attractive, Social and Timely (EAST)". Taking these four elements, we can nudge more secure behaviours online, for example by:

- Easy – people tend to go with the default option so make the default option a decent baseline of security (for example, in terms of password complexity). Make messages as simple as possible, for example a goal such as 'practice good security online' should be as easy to digest as possible, by breaking it down into basic steps;
- Attractive – draw people's attention with good design, images and colour; use rewards as well as punishments;
- Social – discuss where people are performing well. Focusing on how many people use bad behaviours online only makes others think 'oh everyone else has a terrible password, so it doesn't matter if mine is too!'; and
- Timely – prompt people when they are most likely to be receptive, for example after a widely-reported breach, and not when people are at their busiest. Consider immediate costs and benefits, as immediate impacts and results are most influential. 'Discounting' comes into play here, in which people are proven to be unwilling to spend on unknown outcomes. Help people plan the detail of their response to events to mitigate the gap between intentions and actions.

De Nederlandsche Bank (DNB)

The DNB launched the TIBER initiative (Threat Intelligence Based Ethical Red teaming), the aim of which is to strengthen the cyber resilience of the Dutch core financial institutions against advanced attackers. TIBER aims to improve the cyber resilience of the participants, and it builds on previous experiences by the Bank of England (CBEST). Key to the June 2016 launched programme are: threat intelligence; emulate the best attackers; and collaboratively learn from the findings. This initiative is to be expanded across Europe.

EY

EY's Global Information Security Survey 2015 found that 44% of executives consider employees the greatest cyber security vulnerability in their organisation. Furthermore, 56% of organisations consider employees the most likely source of a cyber-attack – an increase of 12% from 2014. EY believes that educational programmes can help reduce the risk of data breaches. Even basics such as the need for strong passwords and regular changes, are necessary – 63% of data breaches involve default, weak or stolen passwords. Yet, education is only one step in decreasing the cyber risk posed by employees. Organisations also need to incentivise employees to priorities cyber security.

Organisations still primarily rely on traditional methods such as computer-based education, emails, posters and agreements to increase cyber security awareness. Those messages, however, are often neglected by employees. Only a few organisations assess their employees' adherence to data protection requirements through performance evaluation processes. By making cyber security a key performance indicator (KPI), organisations send a clear signal that data protection is an imperative and give employees a vested interest in protecting data.

A strong identity and access management (IAM) strategy reduces this cyber risk by limiting employees' access to sensitive data. IAM involves managing users' online identities and the authentication, authorisation and privileges across IT and business systems. Because 53% of cyber incidents involving insiders result from the abuse of user access rights, organisations must continually ensure their employees' access level matches the needs of their current job roles.

IAM strategies must also address the growing trend of employees using mobile devices, especially their personal ones, to access sensitive company data. 61% use their mobile devices for both personal and work-related tasks, while the great majority receive no training over safely using these devices. With an estimated 50 billion internet-connected devices by 2020, this risk will only increase unless drastic action is taken by organisations.

GO-Science

GO-Science issued a report on "Using Behavioural Insights to Improve the Public's Use of Cyber Security Best Practices", which identified a number of problems for businesses when using the internet, these include: lacking the required expertise to set up technical defences; employees not following the cyber-security policies put in place by the company; and many not even perceiving a risk.

To address the human component of cyber security the report addresses the factors which affect human behaviour in general and in cyber security behaviours specifically. It is noted that there is a specific lack of:

- Reliable data on individual internet users' cyber security actions. What users say they understand and do is not necessarily the same as what they actually do;
- Research on the factors influencing an individual's cyber security practices or lack thereof;
- A theory of human behaviour or a comprehensive understanding of how to change human behaviour in this context; and
- Agreement between stakeholders on the size of the problem, the risks and the necessary behaviours required and therefore the public receives confusing and contradictory messages.

The report focusses on how to motivate the general public to adhere to the Cyber Security Best Practices – 10 cyber security best practices designed following a review of the guidance currently available and a discussion with experts:

1. Use strong passwords and manage them securely;
2. Use anti-virus software and firewalls;
3. Always run the latest version of software;
4. Log out of sites after you have finished and shut down your computer;
5. Use only trusted and secure connections, computers and devises (including Wi-Fi);

6. Use only trusted and secure, sites and services;
7. Stay informed about risks (knowledge, common sense, intuition). Try to avoid scams and phishing;
8. Always opt to provide the minimal amount of personal information needed for any online interaction and keep your identity protected;
9. Be aware of your physical surroundings when online; and
10. Report cybercrimes and criminals to the authorities.

GO-Science compiled three categories of behaviour change theories that examine what influences people's behaviour. These categories are environmental, social and personal:

Environmental influencers

Environmental influences reflect the design of the environment, the physical environment such as the workplace, the work flow and the technology, including economic factors. Good design is fundamental and security practices should be designed in from the start and not shoe horned in at the end. Much of the technical effort in cyber security has been aimed at designing security tools that are easier to use. Good design ensures that security is the default. Visualisations and feedback can be used to inform users of the current system status as the risks they are taking. This information can be pushed to the users to ensure they have sufficient information to make informed decisions at any point in time. Design can also be used to persuade people to behave more securely.

Users carry out cost benefit analysis when deciding how to behave. Incentives influence behaviour and these can be positive (benefits: rewards) or negative (costs: sanctions and punishment). Users will happily ignore the security credentials and risks of a website if economic factors are right. Motivators such as desire for a free product can lead to ill-advised downloads, use of insecure sites and excessive information disclosure.

Research on sanctions for poor security behaviour highlighted some surprising findings – higher penalties were not associated with more secure behaviours. Likelihood of detection was a more reliable predictor of behaviour than the severity of the consequences.

Social influencers

Users are influenced by the people around them – friends, family, colleagues and fellow citizens. Other peoples' beliefs and behaviour strongly influence our own, the majority of people will conform to the 'social norm'. within the workplace, organisational culture influences our perceptions of acceptable behaviour. Leadership in general has been found to be a key component of security culture – management must be seen to behave securely.

Personal influencers

In terms of knowledge, users cannot comply with best practices if they do not know what it is or what risks/attacks to look out for. This is particularly problematic within cyber security where the nature of attacks appears to be constantly changing. People sometimes rely on heuristics, or mental shortcuts that allow them to make judgments quickly and effectively. These rule-of-thumb strategies shorten decision-making time and allow people to function without constantly stopping to think about the next course of action. While heuristics are helpful in many situations, they can also lead to biases.

The communication of consistent and useful information is a necessary prerequisite for behaviour. However, it should be stressed that information alone is not necessarily sufficient to encourage behaviour change. Studies have shown that despite awareness campaigns and training, poor cyber security behaviours persist. So far knowledge has not been found to be a good predictor of cyber security behaviours. While information rich campaigns may inform people, they may fail to motivate change.

Intuition

Intuition highlights firms like Equifax could have used a Thaler-style nudge to tighten up their IT practices. The Equifax breach – one of the worst data breaches in history – arose because the company failed to update its software, and a big reason for this is because it lacked incentives to do so.

Nudges should simple, regularly enforced messages that grab the attention of users and highlight incentives that tap into the human instinct to align with others. 95% of security breaches involve human error, according to IBM statistics. 49% of companies surveyed by the Ponemon Institute report that their security training programmes fail to deliver behaviour change.

In 2016, the European Commission ran an experiment to better understand the effect of nudges on online behaviours. Over 5000 people had to make a purchase on a mock online store while in the background, scientists tinkered with a range of potential behavioural nudges. They wanted to prove that a simple change to the “choice architecture” could nudge online behaviours in the right direction. The nudges came in the form of warning messages, displayed visually at the beginning of the experiment. The effectiveness of these messages was tested by measuring their impact on a defined set of behavioural measures, including whether shoppers used a secure password and whether they remembered to log out. The scientists found that timely messages informing shoppers that they could easily protect themselves and giving cleat instructions on how to behave safely had a positive impact on all the behavioural measures-proving that the nudge worked.

However, cyber security nudges are not limited to warning messages. For instance, awareness programmes that position safe cyber security practices as the social norm will promote safe behaviours by tapping into the deep-seated human need to conform. Nudges can be an effective and inexpensive way to promote cyber security best practices, reducing the likelihood of wayward behaviours manifesting themselves as an expensive security breach.

PWC

PWC suggests several nudges which can encourage secure employee behaviour online, without a large cost.

- Add a permanent button to a reporting form on everyone’s desktop. Alternatively, the organisation's IT department could be augmented to give the option of reporting a security breach as the first option.
- A nudge may appeal to employees' social nature and biases, such as using campaigns which emphasise how frequently others are reporting security incidents, thereby triggering a bandwagon effect which encourages reporting.
- Another option PWC clients are exploring is gamification - making desired security behaviours fun or competitive could be encouraged if legitimate security incident reporting feeds into leader boards or points.

Noted that it’s not always going to be simple to nudge security. The approach used involves trialling nudges in specific business areas, and comparing impact against controls groups who are left untouched. This is to allow for any tweaks or re-designs which may be required, depending on these results. For instance, the example above which communicates how frequently others are reporting security incidents could have a perverse effect as individuals think that they don’t have to report security incidents because others will do it for them. Testing will allow such effects to be observed and when success is found, it can be replicated across organisations.

Security nudging is one tool for encouraging good security behaviour, and should sit alongside efforts to challenge beliefs and underlying assumptions. These assumptions are key to changing security behaviours ("I wouldn't get phished", "I don't need to stop that person I don't recognise"). As one tool in the box, nudges can be simple, and cheap, and are proven to have big fast acting impacts when they effectively tap into the decision environment.

Norton

Norton reports that cyber security around the office begins with education and training – education in best practices and training in how to best execute those best practices, as well as making them a daily habit. Some key areas include:

- *App updating*: The main way that hackers are going to find a way into your system is through outdated apps with known exploits. Make sure co-workers and employees know to update their apps as soon as the update is available.
- *Password control*: The best solution is a password management application. This holds all of your passwords in one place, allowing people to generate strong, random passwords. They then only need to remember one strong password to unlock the app itself. Barring that, use strong passwords, only use them once and never store them on a post-it note on the monitor.
- *VPNs*: Especially for a business, VPNs aren’t optional. These encrypt all traffic leaving your computer until it reaches its destination. If someone somehow manages to get in the middle of your traffic, all they will have is encrypted junk data. It’s not enough to have a VPN, people must make sure they’re actually using them.
- *Cyber security as part of basic training*: Educate all current employees at once and all new employees coming in with the same best practices. As best practices become updated, update your training and corral the team to make sure everyone continues to be on the same page.

Beyond education

- *Compliance programmes*: Make changing passwords a regular task. Make sure everyone is doing what they need to do to keep their passwords secure.
- *Rewards programmes*: Offer rewards for employees who find ways to improve cyber security around the office. Don't look to spot check your cyber security. Look for ways to make small, but significant tweaks to what you're already doing.
- *Accountability programmes*: Encouraging employees to implicate one another for not following best practices will just erode trust. However, encouraging employees to gently hold one another accountable will ensure compliance with best practices.

REDSCAN

REDSCAN suggests not to:

Click on unverified URLs or email attachments

Preventions:

- Copy and paste URLs into a browser rather than clicking on them directly
- Don't share important details over the phone or via email
- Scrutinise emails for giveaway signs like spelling errors or inaccuracies
- Check that the sender and reply addresses of an email are the same
- Seek secondary reassurance if asked to do something that has a financial impact
- Conduct a simulated social engineering attack to test employee awareness

Set weak passwords

Preventions:

- Enforce a strong corporate password policy utilising uppercase, lowercase and special characters
- Encourage users to create unique passwords by sharing awareness of password generation techniques and tools
- Leverage security information and event management (SIEM) to monitor for brute-force attempts and suspicious network activity

Possess unnecessary network permission

Preventions:

- Enforce a strict access policy that limits user privileges as far as possible
- Encourage system administrators to only turn on admin rights when needed
- Regularly review and update credentials to reflect job changes and leavers
- Ensure that remote employees, subcontractors, third-party vendors and partners are included in administrative policies
- Avoid or limit instances of employees sharing generic account credentials

Download harmful files and software

Preventions:

- Raise awareness of downloading files from untrusted sources
- Block access to torrents and suspect websites
- Where possible prevent users from downloading and/or installing new software
- Conduct daily system backups
- Perform regular vulnerability scans to detect out of date software and applications

Connect removable devices to company networks

Preventions:

- Operate a separate, segregated Wi-Fi network for use by guests and employees using personal devices
- Raise awareness of downloading files from untrusted sources
- Limit the number of available USB ports to prevent users from plugging devices into networked systems
- Use a SIEM tool to detect and alert when USB drives are connected to a host
- Utilise endpoint protection to hunt for, detect, and eradicate threats from hosts