# 4 STEPS TO IMPROVE CYBER HYGIENE

## CYBER FACTS & OBSERVATIONS

*Data protection has never been a more significant concern for businesses and individuals. Across the world increasing efforts have been made to create laws and regulations to help safeguard people's personal data as digital transformation projects progress within organisations and governments.*

*The need to treat this data fairly and to protect it is now paramount - **the reputations and fortunes of businesses and senior executives depend on it.***

## CYBER SECURITY IS, OR SHOULD BE, ON ALL BOARD AGENDAS

**What aspect of data protection is highest on the list?**

> ***"When the Information Commissioner's Office (ICO) ran a recent survey on peoples' views about information rights, they found (perhaps not unexpectedly) that Cyber security came out as the top concern."***

One reason for this is likely to be the series of high-profile Cyber incidents that have directly affected large numbers of people and led to headlines that have brought the issue to the attention of many, many more.

## CYBER SECURITY BREACHES IN THE NEWS

**The security breaches that have made the headlines hold valuable lessons for future data protection within organisations.**

### STARWOOD/MARRIOT

The ICO's investigation into the Starwood/Marriot breach found that Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems. Resulting in a circa £99million fine.

### BRITISH AIRWAYS

In the BA breach, the ICO found that information (including login, payment card, and travel booking details as well names and addresses) was compromised by inadequate security arrangements at the company. The ICO announces its intention to fine British Airways.

### EQUIFAX

Similarly, the Federal Trade Commission (FTC) in the US found that Equifax, in their breach, failed to implement and maintain a comprehensive security programme, giving examples such as:

- They didn't check to make sure employees followed the patching process
- They failed to detect that a patch was needed because they used an automated scan that wasn't properly configured
- They didn't have adequate controls on the basics, and rather damningly the FTC concluded.

*It's almost unthinkable not to implement those fundamental protections.*

EDGE IT GROUP LTD

FUTURE THINKING TECHNOLOGY

Huntsman®
Defence-Grade Cyber Security

## CYBER RISK AT BOARD LEVEL

The view of data protection and Cyber risk 'from the top' is a complex one. The way information is used and collected, legal concerns about privacy notices and reliance on third parties all complicate what can already be a daunting technical discipline.

### MINIMISE LIKELIHOOD OF FINES

If you can reduce the exposure or vulnerability to Cyber security breaches, you can make them less likely and with less impact. Given a fixed amount of personal data at risk, or a set cost to investigate, the fewer breaches that have to incur costs the better. Ideally of course, you want no breaches at all.

### MINIMISE THE IMPACT OF BREACHES

When a breach occurs, the scale or impact of the breach, the amount of attention it attracts, and the size of the fine (and other costs) are linked. So, ensure you have controls in place to limit information access and data flows, then ensure issues can be detected quickly, ideally as they occur, so that you can stop unauthorised transfers in their tracks.

Partition data sets so that when a compromise exposes data it is not the full range of information held, but a smaller and less sensitive subset.

### MINIMISE THE EMBARRASSMENT

If data has been stolen or corrupted, your organisation will come in for criticism; but the extent of this will depend on the nature of the breach; how fallible you have been and how lax the controls were that were in place.

It's not just the "optics" of the breach; there is less blame attached when falling victim to a highly complex breach conducted by a well-resourced and determined attacker, than there is for allowing a trivial attack or control failure to result in a significant data loss. You might have failed, but there may still be room for sympathy as well as condemnation.

## KNOW YOUR CYBER POSTURE AND RISK

No set of security controls is perfect; there will always be holes, known vulnerabilities that haven't yet been addressed or risks that the business has accepted in order to function.

It is important to know what state your Cyber security controls are in so that you can make decisions as to whether the level of risk is acceptable, and so that if a problem occurs, you have some understanding of the decisions that might have caused it. Good reporting and visibility of Cyber security operations is key to avoiding surprises when the worst happens.

**Be transparent.** Don't try to hide or cover up a breach when it occurs.

## TWO TYPES OF BREACH

There are really two categories of breach; two ways in which controls can fail that allow a theft of personal information or a mass corruption of data to occur.

The reason this distinction is important is in the way Cyber defences are arrayed to prevent them (which we will come to) and the way in which they can be anticipated.

### SIMPLE/TRIVIAL (AND MOST EMBARRASSING)

Some breaches come as a result of an attacker, or a malicious insider, or some other technical failure exploiting a basic and obvious control. An attacker might gain access to a system with a default password that wasn't changed, a file might be stored on a publicly accessible and unprotected file store, or in the case of the NHS WannaCry outbreak, an environment might have operating system patch levels that are so far out of date that an attack is inevitable.

Attacks like this are easy to predict. If you have a glaring weakness that is easy to find and easy to exploit, you will get attacked, you will lose data, and it will be your fault. These are situations that can be anticipated.

### COMPLEX/TARGETED (AND MOST DAMAGING)

The more insidious and complex attacks that organisations suffer from are harder to anticipate as they tend to involve long, complex chains of attack (often referred to as a 'kill chain') where a target is identified, researched, probed, then initial access obtained; before the attacker or intrusion spreads around the network or systems to find particular data sets or the most interesting files of personal data.

This type of attack is very challenging, as you must, defend every possible path into the organisation and make sure that all the combinations of ways to access and navigate a network are controlled.

After the fact, there is at least the hope of a trail of breadcrumbs that shows how the attack progressed; but beforehand it is harder to foretell.

This 'kill chain' concept relates to hard-to-predict complex attacks, that string together a series of smaller weaknesses and exploits to gain access, move laterally and steal data. The actual circumstances of a specific breach will be a complex; but the steps taken to achieve it will be, once again, the simple, trivial, easily exploitable and predictable weaknesses we first outlined.

## FOUR STEPS TO IMPROVE CYBER HYGIENE

We've established that businesses need to be able to defend against both simple and complex attacks. Further, that many sophisticated attacks occur through chains of smaller failures that are exploited in sequence.

Making decisions about risk, and understanding this at a business level, means being aware of Cyber risk posture in a way that allows risk management decisions to be open, transparent and defendable.

**Businesses must follow these 4 simple steps:**

### 1) IMPLEMENT THE RIGHT 'CYBER HYGIENE' CONTROLS

Cyber hygiene is about covering the 'low hanging fruit' and making sure that simple security flaws that are well known to defenders and attackers are covered. This means secure configurations for operations systems and preventative controls around types of user activity to reduce risk (on top of awareness training).

The benefit is you have protection in place against the most trivial (and hence embarrassing) breaches, plus you stand a chance of breaking a more sophisticated attack 'kill chain' at one of the intermediate stages as an attack progresses from the initial intrusion.

This was the explicit aim of Essential 8 initiative to formalise Cyber mitigation strategies.

### 2) MAKE SECURITY OPERATIONS VISIBLE

Reporting in dashboards or reports on a large number of 'low level' controls is onerous and generates voluminous outputs with too much detail for senior management. A worthwhile strategy is to select a smaller number of key controls as key performance indicators (KPIs) for reporting.

These checks can then be done automatically on a continuous basis, so changes are visible immediately, and the timeliness of issues is properly reflected. This is critical in a discipline where resources are scarce, and the nature of risk continually changes.

**Getting a true picture of risk means:**

- Checking configurations and control status
- Identifying issues and changes
- Measuring numbers of users/systems that are misconfigured
- Monitoring activity that demonstrates ongoing operation (or reports on failures).

Filtering what's most essential and automating the process of measuring performance results in timely reports and quicker decisions when failures occur and gives a better view of cyber posture in real-time.

### 3) CONTINUOUS MAINTENANCE

Whether your Cyber hygiene and security control framework is in the process of improvement as part of a security programme or operational and continuous, the status of controls and configurations needs constant attention. New patches come out all the time, backups happen (or not) daily, users and administrators can receive a phishing or malware-laden messages at any time.

Maintaining operations in a changing environment requires continuous effort that must be optimised and efficient, allowing you to manage by exception while this is going on, the more esoteric, site-specific, or advanced threats that need attention risk being side-lined.

Getting the basics right and not sliding backwards, it's a never-ending job, so doing it efficiently is vital. This frees up time to allow other improvements to be made.

> *"Once you have working controls, and a process to check, audit, or validate that they are operational, then reporting can follow."*

### 4) MEANINGFUL REPORTING

Reporting on what are effectively KPIs for senior managers means looking at performance, trends over time, and changes from one reporting cycle to the next.

This is the way business functions work, and security processes need to operate similarly. This means avoiding listing issues or vulnerabilities in technical language or assigning subjective ratings based on opinion.

It is the process of managing these issues that the business needs to monitor.

Senior executives must be aware of the risks so that if fines are imposed following a breach, the risk decisions that were made are understood and agreed upon by the business.

Making good Cyber hygiene "normal" allows business and security operations to focus on threat hunting, improvement, and supporting the future business strategy rather than continually looking over their shoulders.

## SUMMARY

If the goal of a business is to reduce the exposure and size of fines for Cyber security failures, then the four steps we have outlined here are key.

### 1) IMPLEMENT GOOD 'CYBER HYGIENE' CONTROLS

This is about having robust baseline controls in place to prevent trivial attacks (the most embarrassing and hardest to defend) as well as interrupting the 'kill chains' of more complex threats.

### 2) MAKE SECURITY OPERATIONS VISIBLE

This provides operational visibility of the "state of controls" so issues and exceptions can be managed, and no one is surprised by failures in controls that were assumed to be working.

### 3) CONTINUOUS MAINTENANCE

This is about keeping the various plates spinning, ensuring that ongoing operations are working in an 'effective and efficient' way.

### 4) MEANINGFUL REPORTING

This gives visibility of Cyber posture in a KPI report the business can easily understand, to show that Cyber security is operating in a way that means risk management decisions around budgets, investment and priorities can be made confidently by stakeholders in risk and compliance roles or by business leaders.

### MINIMISE REGULATORY FINES

Good Cyber hygiene means less frequent and less impactful breaches. You avert casual and trivial attacks and make complex, targeted ones harder to mount, requiring investment in zero-day exploits or more detailed intelligence gathering on the part of the attacker.

This, of course, also means less frequent and lower fines. Furthermore, when those breaches do occur you won't be taken by surprise by the state of controls if you have good, clear, continuous visibility of their status and operation.

Having good understanding of the Cyber posture and risk management decisions that have been made, paints a picture of a business that knows what it is doing when the regulators come calling, rather than one that was caught unawares.

With GDPR fines of up to 4% of global turnover being possible, anything that can evoke more sympathetic treatment has a solid investment case.

To reiterate the FTC: ***"it's almost unthinkable not to implement those fundamental protections."***

**For more information on how Essential 8 performs a key role in achieving these objectives, please contact, either Rod Harrington or Andrew Krauze.**

Cabinet Office

Department
for Culture
Media & Sport

National Cyber
Security Centre

GCHQ

EDGE
IT GROUP LTD

FUTURE
THINKING
TECHNOLOGY

0800 808 5270
https://edge.org.uk
enquiries@edge.org.uk