KLOUDWERK

BRIEFING MEMO

CYBER ATTACK

Mainstream media is awash with news about households and corporations hit by online crime. The headlines focus on big name corporations and financial costs in the millions. Board directors are ultimately responsible for a company's successes and failures. They are faced with an array of business-critical topics requiring a course of action they decide. They expect to be fully briefed on complex matters and very basic questions will come raining down hard & fast. **"How good is our security?" or "Are we safe?"**

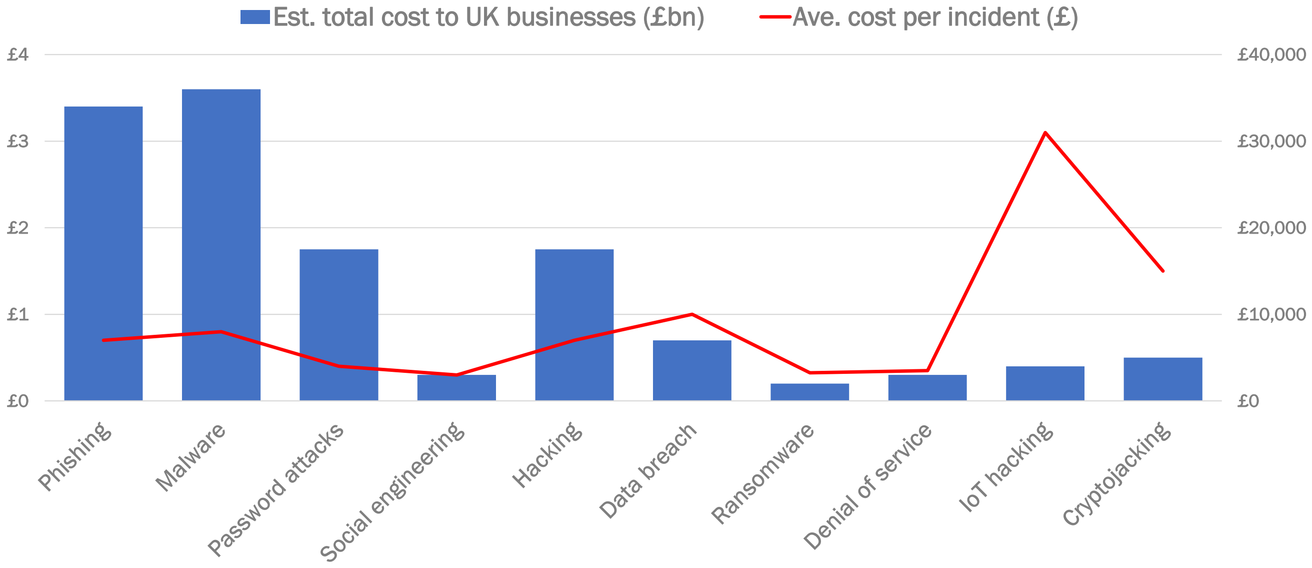
> ***"Everyone has a plan until they get punched in the face." – Mike Tyson***

You may well have to respond to these questions in your capacity as IT Manager or Practice Manager, so let us imagine being the object of a grilling by the Senior Leadership Team when something unexpected happens. Perhaps your company's website has been defaced - it had to be taken offline. Or your systems have been blocked from usage - a denial of service attack. Worse, there has been a breach of your data server - client information has been stolen. Not an everyday occurrence, but certainly a reality and perhaps on-going within your organisation as you read this memo. The best approach is probably answering with high level points about security and so we'll present the information plainly to our audience.

First, there are a lot of valuable insights in the public domain that will help you put the risk of threat into context

In fact, research has found that 20% of small businesses, 24% of medium-sized business and 36% of large businesses now discuss a range of threats at board-level, while the proportion taking additional steps to mitigate the threat doubled from 16% in 2015 to over 40% in 2020.

With cyber attacks steadily on the rise over the last five years, companies of all sizes have not been idle in recognising threats and are addressing the risks. With malware being at the top of the list, nearly 50% of organisations have adopted enhanced security measures to curtail this risk, double in number from five years ago.



Source: Beaming and Opinium, January 2020

Second, let's make the assertion that you have of course taken steps to protect the firm prior to this breach

- ✓ Several common operational reasons have led the organisation to review security approaches. You did so in the course of adopting new digital modes of service delivery, such as moving to online banking, migrating data to new servers or to the cloud, or allowing more flexible remote working among employees or suppliers.
- ✓ GDPR compelled many organisations such as yours to review their approach to securing data from attack.
- ✓ And of course, you have undertaken regular business-as-usual health checks such as risk assessments through internal & external audits, ad-hoc health checks or reviews beyond regular processes, and
- ✓ Last but not least, you have invested in threat intelligence software.

And yet, your walls have been breached and you are under attack. The question then becomes whether or not you have *critical incident risk management* in place, which you do. **So far so good, but you are still firmly under scrutiny by the board members.**

The third message the executive team needs to hear is that the threats evolve and grow

Even more so because you have recently submitted budget request for a substantial IT upgrade. Managing security is a continuous and iterative process, and you have asked yourself the following loaded questions and hopefully answered in the affirmative:

- ✓ Do you know what your estate really looks like?
- ✓ Have you identified vulnerabilities?
- ✓ What could be of interest to an attacker in the first place?

Keep it logical & simple and help them realise the challenges you face. **By this time, we can guarantee you, your audience is glued to your next every word.**

Fourth, help your listeners appreciate the extent of your company's online exposure

- ⇒ It is vast and starts with the email addresses of your organisation's employees.
- ⇒ You have a website or blog and use social media through which you are encouraging as much traffic as you can.
- ⇒ You capture personal information about customers electronically because you have given them the ability to order, book, and pay online.
- ⇒ You have adopted industrial control systems linked to online feeds.
- ⇒ You offer the use of non-work laptop for business purposes (Bring Your Own Device, or BYOD), and
- ⇒ You have recently begun to use externally-hosted web services offered by cloud providers.

In sum, your exposure to the entry point of electronic crime is substantial.

Fifth, give your audience a flavour of the methods used in electronic crime

One can suffer *accidental* breaches as well as ones *perpetrated intentionally*. Moreover, there are *known* breaches versus hidden as yet *unidentified* attacks happening as you speak. In order of priority of incidence and degree of disruptiveness, here are some examples:

⇒ Companies receive fraudulent emails, and employees are being directed to fraudulent websites.

⇒ Outsiders are impersonating the organisation in emails or online.

⇒ The unauthorised use of computers, networks or servers by outsiders has resulted in viruses, spyware, malware, or ransomware being planted.

⇒ There are on-going Denial-of-Service (DoS) attacks which are being deflected.

⇒ There are reports of hacking or attempted hacking of online bank accounts.

⇒ You have disciplined staff who were identified as using computers, networks or servers without authorisation.

In sum, the variety of attack means is very broad.

Sixth, what are the outcomes of breaches or attacks

We immediately think of an outcome in monetary terms. However, by importance of magnitude the following usually happens prior to any immediate & direct monetary cost occurring:

⇒ Temporary loss of access to files or networks;

⇒ Website or online services taken down or slowed;

⇒ Software or systems corrupted or damaged;

⇒ Lost access to relied-on third-party services;

⇒ Permanent loss of files or money stolen;

⇒ Personal data altered, destroyed or taken; and

⇒ Lost or stolen assets, trade secrets or intellectual property.

Lastly, what are the economic damages that breaches incur

Organisations often overlook certain types of costs of breaches, and so undervalue their true economic impact. There are three types of costs that tend to be underestimated:

- Indirect - loss of productivity when staff can't properly carry out their work.
- Ongoing - the recurring cost of new measures put in place after breach.
- Intangible - reputational damage very directly hits the bottom line.

This last point warrants further clarification. When you are prevented from providing goods & services, your customers switch to alternative suppliers. There will invariably be the need to provide goodwill compensation which is compounded by fines and legal costs. **At this stage, the room is gripped and it's the moment to lay out your IT needs.**

In conclusion, on-line security is the broader practice of defending IT assets from attack

Your IT assets are threefold: information, network, and applications. Each requires dedicated policies & measures. The motivations of perpetrators stretch from enthusiast curiosity to economic gain, terrorism & warfare. Pockets funding the industry of hacking an electronic system through the internet are deep.

The standard kill-chain involves the target being surveyed for vulnerabilities, a foothold gained, a weakness exploited, the attack goal achieved. It is therefore key to understand that defences from attack need to be layered and include a range of measures from technology solutions to user education. **Ultimately, a breach happens at endpoints that you as user control, through the actions of your fingertips.**

For further insights please consult our homepage (www.kloudwerk.com)