Cyber Attacks, preparing for when and not if...




Introduction

I'm Antony Gouldstone, an IT professional and Head of ICT Operations with 20 years of experience in the industry. I work for a Fintech organisation in the east of England. Today we are going to talk about the growing problem of Cyber Security and making sure you are ready.

Agenda

Our Story told by the team at the eye of the storm

Statistics – the shocking reality of what is going on

Protecting ourselves

Our Story

So what do the stats tell us?

The statistics tell a worrying story...

- 43% of businesses identified cyber security breaches or attacks in the last year
- £16.1k is the average cost of a data breach for SMEs in the UK
- Up to 88% of UK companies have suffered breaches in the last 12 months. That is lower than Germany (92%), France (94%), and Italy (90%)
- 48% of UK organisations were hit by ransomware in the last year, according to Sophos. This is lower than the global average of 51%.
- 13% of UK organizations reportedly paid the ransom.
- 32% of UK companies have cybersecurity insurance that doesn't cover ransomware.

The statistics tell a worrying story...

- One in every 3,722 emails in the UK is a phishing attempt (20% higher than the global average)
- One small business in the UK is successfully hacked every 19 seconds
- Every day, there are 65,000 attempts to hack SMEs, around 4,500 of which are successful
- 33% of UK organisations say that they lost customers after a data breach
- The average remediation cost of a successful ransomware attack to UK enterprises is $840,000
- Just 31% of UK organizations have done a cyber risk assessment in the last 12 months

Now the legal bit, the data sourses 2020...

carbonblack.com/threat-research/

hiscox.co.uk/sites/uk/files/documents/2019-04/Hiscox_Cyber_Readiness_Report_2019.PDF

hiscoxgroup.com/news/press-releases/2018/18-10-18

csoonline.com/article/3440069/uk-cybersecurity-statistics-you-need-to-know.html

itgovernance.co.uk/data-breaches

news.sophos.com/en-us/2020/05/12/the-state-of-ransomware-2020/

infotech.co.uk/blog/35-cyber-security-stats-to-make-you-serious-about-data-protection

itgovernance.co.uk/data-breaches

“Until you have experienced something like this, you don’t realise just what can happen, just how serious it can be.”
"I had no intuitive idea on how to move forward.”

Maersk CEO Soren Skou on how to survive a cyber attack - Financial Times, 14th August 2017

Protecting Ourselves

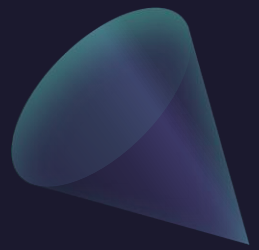
Prevention is always better than a response

People

- Training is key for everyone
  - Ensure that everyone has completed training that covers at least the basic level of understanding
  - Ensure that your IT Teams are trained and practiced on what to do in case of compromise
  - Work with local groups like Cyber East, ECRC, and the Police
- If you are in a compromise situation, remember the welfare of your people. When dealing with these situations, day and night merge into one. Even during these extreme and demanding times you still have a responsibility for the welfare of people

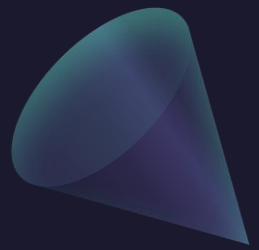
Process

- Cyber Security must be a strategic concern
  - Cyber is not just a problem for the IT department to deal with. To be successful it takes an effort from all to stay in front.
  - Do your board know and understand what is going on when it comes to cyber?
  - Do you have a cyber risk assessment? If not why not
  - Response plans are important but practicing them is essential. Train hard, fight easy



Technology

- Layer up, don’t rely on a single solution
- Ensure your protection levels are appropriate
- Speak to your local policing team about the support they can give
- Patch your vulnerabilities, if you don’t you are leaving a door open.
- Patching is not just about your operating system. You have to apply this to your whole software and hardware stack.



Summary

The cyber threat landscape has and is changing all the time and we have to adapt to it. Remember to equip your teams to deal with the challenges thrown at them. Finally, don't just create and file your policies and playbooks. They must be living breathing documents.

Thank You For Listening

Any Questions?