AN INTRO TO

Preventing Cyber-attacks

In Manufacturing

Security Consultant

IMATIK, London

A Publication of

Table of Contents

CHAPTER ONE

Introduction

Cyber Security Breaches: It's not if, but when.

Anonymous

1

Hackers love the Manufacturing Sector. Here's why.

Statistics taken from the manufacturers' organisation EEF on cyber security issues in the manufacturing sector

- 45% of manufacturers believe that they do not have the right tools to ensure cyber security
- 12% of businesses have no process measures at all to mitigate the cyber threats
- The manufacturing sector is the third most hit by cyber-attacks in the UK

As a result of this trend, 59% of manufacturers have been asked by a customer to demonstrate the robustness of cyber-security processes.

In the interest of full disclosure, at IMATIK, we like to a humorous spin on our work! Here are 10 quick points to enhance your protection in 2020.

2

CHAPTER ONE

Preventing Cyber Attacks In Manufacturing

10 Steps

1

The P Word… PEN test

A penetration test, also known as a pen test, is a simulated cyber-attack against your computer system to check for exploitable vulnerabilities. When's best to have it? Before or after you invest?

1. Before, so you know where to focus
2. After, so you can test your investments

When you leverage a partner to fulfil a PEN test; it's typically a conflict of interest for the same partner to also provide your solutions.

☐ Hire a PEN tester before investing
☐ Hire a PEN tester after investing

2

The Other P Word… Passwords.

81% of hacking-related breaches leveraged either stolen and/or weak passwords. Therefore, step one, is MFA. Manufactures have their fair share of weird and wonderful applications so be sure to use a versatile solution that works well with all of your apps.

- ☐ Do you have an MFA enabled for all apps, all devices and all locations?
- ☐ Do you prevent the use of common passwords?
- ☐ Do you require hard to guess passwords?
- ☐ Try: https://haveibeenpwned.com/ to see if your personal/corporate credentials have been leaked

3

The A Word… Access (remote)

The ability to connect remotely to your corporate network can be a major advantage for business efficiency. Given manufacturers typically have clients and suppliers on a global scale; it is essential users have the right access, at the right time.

Do you allow remote access?

- ☐ Have you enabled multi-factor-authentication for remote sign-on?
- ☐ Is your data encrypted?
- ☐ Do you have a robust firewall and VPN?
- ☐ Do you frequently review server logs to monitor remote access and any unusual activity?
- ☐ Do you frequently delete any remote access privileges once they are not needed?
- ☐ Is your firewall and VPN software patched and up-to-date?

4

The S Word… Staff

Human error is the leading cause of data breaches. Each staff member has a responsibility to uphold the security of a business. To make matters worse; training everyone about security is not an easy task… Our two favourite tests are email phishing and quick 5 question surveys.

So how do you get people to listen? The three S approach. Sympathise, Sponsorship and Strike.

Sympathise, tell them you know that it's a pain in the arse and that you appreciate they'd rather be getting on with something more important.

Sponsorship, if the CEO or executive management is behind it's a hell of a lot easier.

Strike now. While the iron is hot. Don't wait for 2 weeks. Do it when they're venerable, they've just been caught, use that to your advantage.

- ☐ Can staff report suspicious emails quickly and effectively?
- ☐ Do you have the correct onboarding / offboarding processes in place?

5

The M Word... Mobiles

In 2014, Kaspersky Lab detected almost 3.5 million pieces of malware on more than 1 million user devices. And as reported by IT Web, the number of new malware programs detected each day has reached over 230,000--many of which target mobile devices.

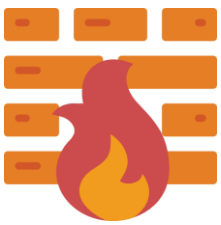
- ☐ Can mobile devices be remotely wiped?
- ☐ Is the data on the mobile device encrypted?
- ☐ Do you apply appropriate restrictions on a mobile device?

6

The F Word... Firewall

Firewalls have been a first line of defence in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

- ☐ Do you have firewalls installed at every point where your computer system is connected to other networks, including the Internet?
- ☐ Are your firewalls fit for purpose?



7

The D Word... DNS

80% of malicious URL's are legitimate sites that have been compromised. A new malicious URL pops up every 2 seconds.

The manufacturing sector often needs to facilitate the very strangest of requests. My personal favourite: “How to lubricate my large machinery?”. DNS protection is often one of your first lines of defence. Most companies do not secure their DNS, but securing your DNS is one of the easiest ways to secure users inside and outside of the network.

- ☐ Do you protect your DNS?
- ☐ Do you secure ‘off-network’ users?

8

The S Word… Supervise

Can you see it? No. Well, how can you secure it then? Do you know what apps are being used in your environment? Most companies have a couple of provisioned file-sharing application. What humours me is the shocked look on people's faces when they trial our solutions to find 40 different file sharing applications being used inside their corporate network.

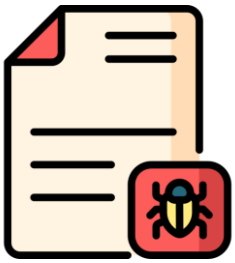
- ☐ Do you monitor what applications your employees are using?
- ☐ If so, do you apply the appropriate restrictions?

9

The V Word… Virus

AV is important but it should be treated as part of a larger solution. AV is your final line of defence. Antivirus software is a computer program used to prevent, detect, and remove malware.

- ☐ Has your anti-virus software been configured to check all mediums (USB memory sticks, flash drives, removable disk drives (CD, DVD, blu-ray), hard drives, emails, web sites, files downloaded from the Internet) for viruses?
- ☐ Is a procedure for automatically updating the anti-virus software in place?



10

The P Word... Policy Enforcement

This is a big concern for manufacturing. Why? Intellectual property, designs, processes, floorplans - hackers want to know your competitive edge. One of the simplest ways to mitigate the risk of data breaches is to limit the information that staff have access to.

Access controls ensure that staff can only view information that's relevant to their job. For example, someone in marketing must be able to view contact information for those who have signed up for a service, but they won't need access to, say, HR files and payroll data.

Walling off those parts of the system ensures that staff can't compromise that data, either accidentally or maliciously. It also protects organisations should a criminal hacker break into an employee's account, as they will only be able to view a select amount of data.

DISCLAIMER

Disclaimer: IMATIK cannot provide any assurance that this checklist will be suitable for your particular needs and neither IMATIK nor any IMATIK employee will be liable on any basis for any consequences arising from your use of this checklist.

IMATIK

Cyber Security Specialists

A Powerful Portfolio, Integrated Seamlessly

Discover the power of simple, effective
cloud security, backed by Cisco's Talos.

LEARN MORE

IMATIK.