CYBILITY

Demystifying Cybersecurity

# Will your organisation be collateral damage in the next cyber attack?

Briefing for executives, non-executive directors and trustees
regarding the increased cyber threat due to Russia's invasion of Ukraine

The main facts you need to know:
What is the threat?
Why should we care?
What can you do about it?

# WHAT IS THE THREAT?

The fight against cyber crime raged behind the scenes for years.  Unknown to many, attackers increased their reach into organisations across the world.

There's a real concern that Putin's physical invasion of Ukraine could escalate into cyber war affecting the daily lives of people far from the conflict zone.

This is especially true once the criminal groups and hacktivists pick sides and attack with the invisible weapons of war.

# What are hacktivists?

Hacktivists are digital vigilantes; rebels with a cause.

Heroes or villains? That depends on which side you're on.

The hacktivist group **Anonymous** called for hackers to unite and carry out cyber attacks against Russia - particularly against the disinformation campaigns to their citizens.

The hacktivist group **Conti** rose to Russia's defense.

# Why should we care?

Cyber attacks in the digital world can have physical impact in the real one including:

- Preventing customers from accessing your services due to a denial-of-service attack or website defacement
- Irretrievable data loss due to ransomware or a wiper
- Reputation damage due to 'doxxing' (when data is stolen and published online)

Your organisation's stance on the war in Ukraine could make it a target for hacktivists and others.
Attackers could inadvertantly take your organisation down whilst attacking your suppliers and cloud services, e.g. Amazon Web Services, Microsoft Azure, Google Cloud Platform and so on.

# Russian-attributed cyber attacks - Past

**BlackEnergy (2015) and Industroyer (2016):** shut off Ukraine's electricity grid, and many places lost power.

**NotPetya (2017):** ransomware attack that targeted Ukrainian financial, energy and government sectors, but affected other European and Russian businesses. Many are still paying the costs of that today.

**BadRabbit (2017):** ransomware attack that disrupted Kyiv's metro, Odessa's airport, Russia's central bank and media outlets.

**Website providers (2019):** targeted Georgia and some of their website providers. The website provider's customers had their websites defaced, including governments, courts, and media organisations.

# Russian-attributed cyber attacks - 2022

**HermeticWiper (Feb 2022):** the attack involved destructive malware that deletes or corrupts data, and has been detected in Ukraine, Latvia and Lithuania.

**Sunseed malware (March 2022):** Belarus based groups used a [likely] compromised Ukrainian armed service member's email account to target European government personnel responsible for managing Ukrainian refugees.

**Phishing and DDoS attacks (Feb, March 2022):** several attacks from groups based in Russia and Belarus, targeting Ukrainian and Polish government and military organisations. A China-based threat actor targeted European organisations with messages related to the Ukrainian invasion.

# What can you do?

The National Cyber Security Centre's recommendations are great; but long.  Get started with these cyber security fundamentals:

## Incident Response Plan

Don't have one? Create one!

## Passphrases

Three random unrelated words. They are long, strong and harder to crack than passwords.

## Backup and Test

Copy your data to an offline external hard drive and test it to ensure you can recover

## Anti-malware software

Install it, update definitions daily and continually scan for threats.

## Multi-factor authentication

Enable it everywhere, to make it harder for attackers to invade your accounts!

## Updates

Install software updates and patches on operating systems, mobile apps, and smart devices as soon as prompted.

## Stay up to date

Follow threat intelligence reports to respond to new threats quickly.

For more on these, check episode 2 of Cybility Savvy: How can we be cybersmart?

info@cybilitysavvy.co.uk | cybilitysavvy.co.uk

# You can also

Listen to this episode:

cybilitysavvy.co.uk

Watch this episode:

cybility.tv

Like and subscribe to stay up-to-date

Reach out to us at Cybility Consulting, to learn how our services can help you to protect your organisation.

CISO Advisor
Virtual CISO
Gap analysis
Tailored education and awareness, inc. mentoring

CYBILITY SAVVY

☎ +44 208 040 2846

✉ info@cybilitysavvy.co.uk

🌐 cybilitysavvy.co.uk