



## Cyber Security - 101

Who is the latest company to be breached, or what new ransomware do we need to be aware of? It's an ever-changing story, making headlines online and in the news daily. Often the businesses that make the headlines are large multinationals that have invested heavily in cyber security and have a team of cyber security experts to protect their businesses. So how are small and medium businesses supposed to keep up? The worrying fact is that while the large corporate organizations make the headlines, millions of small to medium enterprises (SMEs) are falling victim to cyber-attacks annually.

In 2023 there were numerous high profile data breaches within the mortgage industry. This trend is continuing into 2024:

- In October, mortgage loan servicer Mr. Cooper struggled for weeks dealing with a cyberattack that eventually caused the leak of sensitive information of nearly 14.7 million people.
- In November, Fidelity National Financial was hit with ransomware, delaying home purchases across the U.S. for days.
- In December, another title insurance company, First American, confirmed it was dealing with a cyberattack.
- In January LoanDepot filed documents with the Securities and Exchange Commission confirming that its systems had been encrypted.

NAMFS recognizes the dangers that cyber security attacks pose to our industry and so we have created a cyber security focused article that can help to keep your business safe, while conducting business online. Informing our members of the dangers that exist and providing insights on how to “go beyond the basics” will enable your business to implement some basic but effective controls in the fight against cyber-attacks.

### **1. NIST Cybersecurity Framework 2.0:**

When looking at your cybersecurity posture a good place to start is with a recognized industry standard framework. On 26th February 2024, the National Institute of Standards and Technology (NIST) released a major update to its Cybersecurity Framework (CSF) which has been widely adopted by organizations to help them in managing and mitigating cyber risks over the past decade. The

updates to the CSF (v2.0), are the result of years of discussions and public feedback, aimed at enhancing the framework's utilization and applicability across various sectors.

The framework now encompasses six key functions:

- **Govern:** Steer and oversee your organization's cybersecurity strategy and policy.
- **Identify:** Understand the cyber risks to your business operations.
- **Protect:** Implement safeguards against identified risks.
- **Detect:** Identify potential cybersecurity attacks and breaches.
- **Respond:** Address and manage detected cybersecurity incidents.
- **Recover:** Restore operations affected by cyber incidents.

One of the most significant enhancements in CSF 2.0 is the introduction of the Govern Function. This new function underlines the importance of cybersecurity risk management governance, placing it at the forefront of an organization's cybersecurity strategy. It emphasizes that cybersecurity is not just a technical issue but a critical enterprise risk that demands the attention of those in senior leadership roles. The Govern Function aims to ensure that cybersecurity risk management is an integral part of the organizational strategy, aligning with other critical business considerations such as financial stability and reputation.



Figure 1: Steps for creating and using a CSF Organizational Profile

NIST Special Publication (SP) 1300 is a guide for small-to-medium sized businesses (SMB), specifically those who have modest or no cybersecurity plans in place, with considerations to kick-start their cybersecurity risk management strategy by using the NIST Cybersecurity Framework (CSF) 2.0:

[NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide](#)

This is all well and good, but if you are a vendor focusing on growing your business and supporting new and existing customers what can you do to prepare your business against a data breach. The good news is that there are several quick wins that are quick and easy to implement with minimum costs involved.

## **2. User Education:**

A good approach to cyber security will always start with your people. Good employees are key to running a successful business and they are key to protecting your business.

Almost all successful cyber breaches share one variable in common: human error. Human error can manifest in a multitude of ways, from failing to install software security updates in time to having weak passwords and giving up sensitive information to phishing emails. Even as modern anti-malware and threat detection software have grown more sophisticated, cyber criminals know that the effectiveness of technical security measures only goes as far as they are properly utilized by humans. If a cyber-criminal manages to guess the password to an online company portal or uses social engineering to get an employee to make a payment to a bank account controlled by the cyber-criminal, there is nothing that technical solutions can do to stop that intrusion.

Since human error plays such a vast role in cyber breaches, addressing it is key to reducing the chances of your business being successfully targeted. It also allows you to protect your business from a far wider range of threats than any single technical solution could - and can potentially empower your workforce to actively look out for and report new threats they may encounter. Some tips to consider when implementing Human Risk Management (HRM) systems:


- Make training short & engaging — Use short video training courses to engage staff
- Cover the essentials — Be sure to cover key security topics
- Train staff regularly — Monthly training keeps knowledge fresh in the mind
- Avoid technical jargon — Many employees won't understand industry terms
- Replicate common phishing threats — Test staff against scams they're likely to face
- Deploy regular phishing simulations — This helps monitor risk without overkill
- Cover core policies — Make sure your policy library includes the essentials
- Keep policies up to date — Review and update policies each year
- Measure the impact — Track training performance and simulations over time

## **3. Password Management:**

Everyone knows that you should not reuse the same password when logging into different systems and that all passwords should be strong, but what do we mean by strong? The table below shows how the length of your password and the complexity used has a direct impact on the time it takes to hack an account. If you use full complexity of uppercase, lower case, numbers and symbols and your password is 12 or more characters then it is going to be difficult to hack.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

**TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023**

 [Learn how we made this table at hivesystems.io/password](https://hivesystems.io/password)

Any passwords that fall into the purple and red categories in the table above can be hacked within a short period of time and are susceptible to attacks. It is difficult to follow password best practice guidelines when you have so many systems to login to and hundreds of usernames and passwords combinations to remember. The only way to effectively manage passwords is by using a password manager. There are many types of password managers available, some of which provide free accounts for personal use. Once you become familiar with using a password manager, you will wonder how you ever managed without one. All you will need to remember is one strong master password. The rest will be securely managed in your password manager vault.

#### 4. Multifactor Authentication:

Moving on from password management, the next area to consider is Multi-Factor Authentication (MFA). MFA takes password management to the next level and combines three components to make logging into systems more secure:

- **Something You Know:** Like your password.
- **Something You Have:** A physical thing, like your phone or a special key.
- **Something You Are:** A unique trait, like your face, voice or fingerprint.

Imagine having a door with not one, but two locks. Multi-factor authentication (MFA) is the digital equivalent of this security upgrade. By requiring multiple forms of verification, such as a password and a fingerprint scan or a one-time code sent to your smartphone, MFA adds a robust layer of protection to your online accounts. Even if a cybercriminal manages to crack your password, they won't get past this second barrier. From your email accounts to your finances, enabling MFA on all your devices is essential. Who wouldn't want an extra layer of security?

There are several well-known and reputable companies that offer MFA for free. Both Microsoft and Google have an authenticator application that can be downloaded and installed on your smart phone for free. You can also use functionality within password managers as your MFA client. Regardless of how you implement MFA you should also look to turn it on and if a website or system does not have MFA enabled you should think twice before storing any sensitive or PII data.

## 5. Backups an Essential Part of a Cybersecurity Strategy

We use backups in all aspects of everyday life. The spare key for the front door, or the spare tire in the trunk, just in case we get a flat. We should consider backups for our data in the same way, an essential component in protecting our data, just in case.

Cyber resilience is all about preparing for when you are impacted by a cyber event. It's no longer considered a case of "if", but rather "when". When a cyber incident occurs, you want to be prepared and one of the best ways you can prepare is to have robust backups of your data. Many organizations make the mistake of assuming that their data is backed up. The first thing you should do is confirm how often and where your data is backed up. If it turns out that your data is not backed up then you should assess what is your most critical data and how regularly should you back it up. Once you have decided on a backup schedule and location you should then ensure that you carry out a regular exercise to test that you can easily restore data.

The day you have a cyber incident is not the first time you want to be testing your backup restore procedures. Instead test it once or twice a year and ensure that you, or your IT provider are comfortable with the process. You never know when you may need to restore your data.

In the digital age, data is one of the most valuable assets for individuals and organizations. As cyber threats continue to evolve, protecting this data becomes increasingly critical. One of the most reliable defenses against data loss is a robust backup strategy. Many organizations believe that data is automatically backed up, but this is not always the case. The first step in creating a backup strategy is to identify your data and then determine if all critical data is backed up.

Data can be lost due to various reasons, including hardware failure, accidental deletion, or natural disasters. Regular backups ensure that a copy of your data is preserved and can be restored, maintaining business continuity and personal data integrity.

Ransomware attacks, where hackers encrypt data and demand payment for its release, are on the rise. Backups provide a safety net, allowing victims to restore their data without succumbing to ransom demands.

**Competitive Advantage and Reputation:** Companies that quickly recover from data loss incidents minimize downtime, retain customer trust, and maintain a competitive edge in their industry.

Incorporating regular backups into your cybersecurity strategy is not just a best practice; it's a necessity in safeguarding against the myriad of threats in the cyber landscape. By doing so, you ensure that your data remains secure, accessible, and recoverable, no matter what challenges arise.



Information provided by:

Michael O'Conner  
Chief Information Security Officer  
moconnor@nexgencyber.ie