Towerwall

Protecting Data Integrity

Michelle Drolet,
Towerwall founder & CEO

WHAT NIST'S CYBERSECURITY FRAMEWORK CAN DO FOR YOU

(Hint: not just for large organizations)

- **Learn what NIST's Cybersecurity Framework can do for you**
- **Build it right with NIST CSF 800-53**
- **Achieving long term resilience with NIST CSF**
- **NIST CSF is not just for large organizations**

Towerwall
Protecting Data Integrity

So what is the NIST Cybersecurity Framework?

The **NIST Cybersecurity Framework (CSF)** provides a set of computer security policies and guidelines for how organizations can assess and improve their ability to prevent, detect, and respond to cyber-attacks. It provides a high-level taxonomy of **cybersecurity** outcomes and a methodology to assess and manage those outcomes.

*In short, the **NIST CSF** helps organizations to be proactive about risk management.*

A security **framework** adoption study reported that **70%** of surveyed organizations see **NIST's framework** as a popular best practice for computer security, but many note that it requires significant investment.

At face value it seems highly complex. However, by partnering with **Towerwall**, we can help organizations address these very fundamental security best practices. This eBook aims to simplify the primary concepts and aspirations proposed by the **NIST framework** covering the following 4 short essays:

1. **Learn what NIST's Cybersecurity Framework can do for you**
2. **Build it right with NIST CSF 800-53**
3. **Achieving long term resilience with NIST CSF**
4. **NIST CSF is not just for large organizations**

We hope you take the time out to familiarize yourself with these important Federal government-backed **NIST** standards. Please don't hesitate to contact us with your questions and concerns.

Sincerely,
Michelle Drolet
CEO, Towerwall
Framingham, MA
michelled@towerwall.com

LEARN WHAT NIST'S CYBERSECURITY FRAMEWORK CAN DO FOR YOU

An invaluable roadmap for InfoSec management

Towerwall
Protecting Data Integrity

The meteoric rise of cybercrime has caught many organizations unawares. Malware has spread from PCs to smartphones, phishing scams have grown more sophisticated, and ransomware is running rampant.

You can hire hackers and botnets, or buy **cybercrime software**, complete with technical support, all too easily. The rapidly expanding Internet of Things is woefully insecure, creating many more access points that can be exploited by hackers.

In the face of this growing threat, we need to find practical strategies that can be employed to mitigate risk and protect our data. One such strategy can be found in a National Institute of Standards and Technology **(NIST)** document called the **Cybersecurity Framework**.

WHAT IS NIST'S CYBERSECURITY FRAMEWORK?

The product of extensive collaboration in the security industry, this document is a constantly evolving **framework** designed to help organizations strengthen their defenses, benefitting the entire community from state governments to banks to retail chains and beyond. It's a comprehensive, flexible guide that presents important principles to help you build the necessary culture to stay ahead in the race against cybercriminals.

ESTABLISHING COMMON STANDARDS

Because everything is interconnected, the architects recognized the need for a collaborative and holistic approach that's inclusive. The **framework** provides a common, accessible set of reference points for everyone from **InfoSec** professionals to executives across industries, helping to strengthen their **cybersecurity** strategies, not just individually, but also collectively.

NIST's framework ensures that everyone is speaking the same language, making it easier to share and discuss tactics, and to plan, deploy, and improve **cybersecurity** strategies.

Whether you're establishing a **cybersecurity** program, or you simply want to strengthen what you already have in place, **NIST's framework** can help. By following it, organizations can get a clear view of the current state of their **cybersecurity**, they can establish targets, identify potential improvements, assess progress accurately, and communicate about **cybersecurity** risks both internally and externally.

LEARN WHAT NIST'S CYBERSECURITY FRAMEWORK CAN DO FOR YOU

An invaluable roadmap for InfoSec management

Towerwall
Protecting Data Integrity

Adoption reached **30%** within two years, according to Gartner, and that's expected to rise to **50%** by **2020**. Broad adoption furthers everyone's understanding and fosters the creation of automated tools and processes to help companies quickly and effectively prove due diligence and compliance through their **cybersecurity** strategy.

MEASURING YOUR EVOLUTION

Just as **cybercriminals** evolve and develop new tactics to uncover fresh vectors of attack, our **cybersecurity** defenses should be agile and constantly improving. The **framework** is a risk-based approach that's broken down into three parts. The depth of detail contained within is beyond the scope of this article, but here's a brief overview:

The **Framework Core** focusses on five functions: Identify, Protect, Detect, Respond, and Recover. They can be adapted for any organization or situation. They're not intended as a path to follow, but rather as a concurrent and continuous set of functions that can deliver a big picture view of the health of your **cybersecurity** strategy.

The **Framework Implementation Tiers** help organizations to characterize their practices. There are four tiers and selection requires careful consideration of risk management tactics, likely threats, legal and regulatory requirements, organizational constraints, and, of course, business goals. The idea is to help organizations to progress from informal, reactive responses to threats, and help them become agile and risk-informed.

The **Framework Profile** empowers organizations to identify opportunities for improvement by revealing the gaps between their current strategy and their target state. It can be configured to encompass security goals and priorities, tempered with business needs and cost-effectiveness.
Ultimately, the **framework** is flexible enough to cater for any industry, providing an effective way to establish a baseline, set goals for improvement, and continuously assess progress.

But there's also recognition that the goalposts are constantly moving. Rather than setting a course for an endpoint, we need to continually ask the right questions and define strategies that adapt to meet perpetually changing threats. By being proactive in our risk management, we can stay one step ahead of the cybercriminals.

BUILD IT RIGHT WITH NIST'S CYBERSECURITY FRAMEWORK

Diving into NIST Special Publication 800-53 for practical advice

Towerwall
Protecting Data Integrity

We've already laid out a broad overview of what **NIST's cybersecurity framework** can do for you, so today we're going to drill into Special Publication **800-53**. Published by the National Institute of Standards and Technology, and based on important research from the Information Technology Laboratory, this publication offers a comprehensive set of security controls to help you protect your data.

The document refers to Federal information systems, but this terminology will be removed in the forthcoming fifth revision, because the advice here is applicable to all organizations.

It may seem dense and inaccessible at first, so we're going to break down some of the key elements and explain their importance.

ESTABLISHING A BASELINE

It's not easy to calculate the business impact of a cyberattack, because there are many knock-on effects that take time to reveal themselves. The latest research from the Ponemon Institute suggests a global average cost of **$3.62 million** for a data breach. The level of potential risk is your starting point in developing and building solid **cybersecurity** defenses.

Before you can select the right set of security controls, you must consider the importance and sensitivity of the data. The **FIPS 199** document explains how you might go about categorizing your systems, taking into account confidentiality, integrity, and availability to figure out if the potential impact of a breach is low, moderate, or high risk.

Having established the potential impact levels, you can select a security control baseline. It's deliberately called a baseline, because it's something to build on.

TAILORING YOUR SECURITY CONTROLS

The guidelines are broad and make certain assumptions that might not apply to your organization, so the next step is to tweak your security control baseline to ensure that it's aligned with your business functions, systems and operating environment. You may be able to drop some controls, but will probably have to add or enhance others.

Part of the aim during this process is to arrive an approach that strikes a good balance between security and cost. There's no such thing as a perfect set of security controls. You must weigh in regulations, emerging threats, new and legacy technologies and systems, plus your business goals, to arrive at the right blend for your organization.

IMPLEMENTATION AND ASSESSMENT

Detailed documentation laying out the design, development and implementation of your security controls is vital for regulatory bodies to be able to audit your efforts. It also provides a sound rationale that can be continually applied for the future, because **cybersecurity** is a travelling cliché – it's not a destination, but a journey.

Being able to refer to this documentation could be hugely valuable for the long haul, particularly if you have a new system to integrate, or your **CISO** resigns, or you hired a virtual **CISO** for the short term.

A common mistake that organizations make is to draft the plan, implement it, and then trust that it's working as expected. Without in-depth, regular assessments you have no idea if your security controls have been implemented correctly, if they're operating as intended, or if they're meeting your expectations for security. Get an outside party with no vested interest to put your security through its paces and don't forget to test your third-party service providers to ensure they meet your standards.

CONTINUOUS MONITORING

You've set a baseline, tweaked it to fit your needs, implemented it and tested to ensure that it's working properly, now you can take it easy, right? Wrong!

Your work is never done when it comes to **cybersecurity** because things change. You might adopt a new system, integrate a new third-party service, or change your business goals. To comply with your legal requirements, you need to be up to date with the latest regulations. And all the while, new software vulnerabilities are being discovered, and hackers are probing your defenses and developing new techniques to gain entry.

At the heart of **NIST's holistic approach** to **infosec** and risk management are two simple ideas – **"Build it right"** and **"continuous monitoring."**

Take your time and create a solid **cybersecurity** foundation, but accept that you'll need to be vigilant for cracks in your defenses and continually make improvements if you want to ensure that your data is truly protected.

ACHIEVING LONG TERM RESILIENCE WITH NIST'S CYBERSECURITY FRAMEWORK

The need for continuous monitoring, effective metrics and skilled workers

Towerwall
Protecting Data Integrity

The laudable aim of the **National Institute of Standards and Technology (NIST)** is to build a common language through a set of best practices and security principles that any organization can apply to combat cybercrime. We've looked at what **NIST's Cybersecurity Framework** can do for you. We've also drilled a little deeper to reveal the importance of solid analysis in assessing your risk and requirements to ensure that you built it right first time.

A solid foundation is a great start, but you also need to implement continuous monitoring and find a way to measure how successful your efforts have been. Because security is a race, rather than a destination, it's vital to keep identifying gaps, making improvements, and validating your activities. To do that, you'll need the right attitude and the right talent.

CHANGE IS CONSTANT

Cybercriminals and would-be hackers are constantly developing new techniques and uncovering fresh vulnerabilities, so defenses must be monitored and updated continually. While the **Cybersecurity Framework** offered up is a great starting point, with lots of useful advice, it's not easy to assess how effective it has been within organizations.

That's the main reason why, at the beginning of the year, the **NIST Cybersecurity Framework**, Assessment and Auditing Act of **2017** was passed into law. It's an attempt to ensure that progress is measured, but establishing metrics to measure the effectiveness of security policies is a tricky business. Different organizations have different priorities.

The **framework** provides a skeleton that you can flesh out with your own organization's requirements, and the metrics you adopt to measure the efficacy of your efforts are no different. If you don't take the time to build a solid set of metrics, then you really don't know if your efforts are paying off.

Later this year, there will also be a major revision to the document, which is available in draft form right now. Collaborators have been working to integrate privacy and cyber controls and align them with **NIST's cybersecurity framework** recommendations. You can currently review and comment on this document, ahead of a final draft at the end of the year.

A VERY LARGE SKILLS GAP

One of the biggest challenges facing any organization that's trying to put **NIST's cybersecurity framework** into practice is the lack of workers with the right skillset.

ACHIEVING LONG TERM RESILIENCE WITH NIST'S CYBERSECURITY FRAMEWORK

The need for continuous monitoring, effective metrics and skilled workers

Towerwall
Protecting Data Integrity

Take a look at the interactive map at Cyberseek.org for an overview of the problem. There were **112,000 InfoSec** analyst job openings last year in the United States, but only **96,870** workers to go around.

Another **200,000** openings requested **cybersecurity**-related skills. Cloud security skills were apparently the hardest to find, with jobs remaining open an average of **96** days. This worrying shortfall has prompted the creation of the National Initiative for **Cybersecurity Education (NICE).** Just as the **cybersecurity framework** creates a common language for discussing security issues and best practices, NICE aims to help you assess workforce skills and identify certification and training requirements.

Many organizations struggle to find people who possess the right knowledge, skills and abilities, and worse, they often can't fully articulate precisely what they need. This is one of the reasons that a virtual **CISO** can be a real boon for an organization trying to get its **cybersecurity** polices on track and recruit an effective team.

SECURITY FOR ALL

Because the **cybersecurity** space is developing so quickly, it's understandable that some of the risks caught some organizations unawares. But ignorance can no longer be used as an excuse. Data breaches and other **cybersecurity** incidents can often now result in regulatory fines and serious reputational damage.

While there seems to be a general acceptance about the level of threat, we are still not seeing the positive action required to nullify it. Verizon's **2017** Data Breach Investigations Report found that **88%** of breaches still fall into one of the nine patterns it identified back in **2014**. The difficulty organizations are having is in validating implementation and building resilience.

The fact that **NIST** is working hard with the wider community to pool resources and knowledge is very encouraging. The importance of this endeavor comes into sharp relief when you consider the bi-partisan cooperation in a generally combative political climate. The government and wider **cybersecurity** community are committed to effecting real change and tightening our collective defenses, but we all need to pitch in.

NIST CYBERSECURITY FRAMEWORK

NOT JUST FOR LARGE ORGANIZATIONS

Small and mid-sized businesses are at most risk and so have greater need

Towerwall
Protecting Data Integrity

The **National Institute of Standards and Technology (NIST)** has been dedicating a lot of time and effort to help organizations improve their **cybersecurity**. We've looked at **NIST's Cybersecurity Framework**, we've talked about how to build it right and the importance of long term resilience.

In this article, we'd like to dispel the erroneous idea that **NIST's guidelines** are just for large organizations.

Cybercrime is a great threat, regardless of the size of your business, but there are compelling reasons that smaller businesses need to be sitting up, paying attention and, most importantly, taking action.

GOING OUT OF BUSINESS

"Small- and medium-sized businesses are drivers of the economy. Statistics show that when [these businesses] are the victim of a cyberattack they go out of business in less than a year," Walter Copan, the President's current nominee for the **NIST** director post, told Science magazine recently.

Sadly, it's true. Big data breaches may make the headlines, but large organizations usually have the resources and resilience to recover, whereas smaller businesses may never recover. Consider that **60%** of all small businesses that suffer a cyber-attack go out of business within six months, according to the **U.S. National Cyber Security Alliance**.

That's a frightening statistic and it highlights the need for small businesses to seek out advice and consider the best plan. If you're inexperienced when it comes to **cybersecurity**, then **NIST's** Small Business Information Security: The Fundamentals is a very good place to start.

"Many small businesses think that **cybersecurity** is too expensive or difficult; Small Business Information Security is designed for them," says lead author, Pat Toth in a **NIST** article.

LOW HANGING FRUIT

For **cybercriminals**, the path of least resistance is often the one they'll take. They won't hack through a clever set of defenses when they can con a password out of someone with administration privileges. By that same token, it's often much easier to gain access to a small business than a large one, because basic defenses are limited or entirely lacking.

NIST CYBERSECURITY FRAMEWORK

NOT JUST FOR LARGE ORGANIZATIONS

Small and mid-sized businesses are at most risk and so have greater need

Towerwall
Protecting Data Integrity

When a Manta poll asked **1,420** small business owners whether they felt at risk of a data breach, a whopping **87%** answered no. To make matters worse, **31%** of small business owners admitted that they have no controls in place to prevent attacks. A lack of proper **cybersecurity** tools and expertise can be disastrous and it often is.

From phishing scams to insecure IoT devices there are risks and vulnerabilities everywhere. No wonder then, that in **2016** when the Ponemon Institute surveyed **600** IT leaders at small and medium sized businesses, it found that half of them had been breached in the previous **12** months. Only **14%** of the companies in the study rated their ability to mitigate cyber risks, vulnerabilities and attacks as highly effective.

WHAT SHOULD YOU DO?

The **NIST** guide we linked above is designed to assist you in running a simple risk assessment, which is always the first step towards understanding your vulnerabilities. The basic principles of the **Cybersecurity Framework** are every bit as applicable to small businesses as they are to large organizations, so think about staff education and information security training, lock down access to sensitive data, encrypt data, monitor and filter traffic, and keep the software you use fully up to date with the latest security patches.

Another vital step to take, which may seem like a lot of work upfront but will most certainly save you a lot of pain if you suffer a breach, is to develop an Incident Response plan and create a Play Book. Having a procedure to follow when the worst happens can be the difference between a manageable problem and the end of your business.

As big businesses tighten up their **cybersecurity** defenses, the risk for small and mid-sized businesses is only going to grow bigger. We're glad to see smaller businesses make **NIST** more of a priority. **NIST's framework** can provide a lot of useful, actionable and repeatable advice, so make sure you take advantage.