



THE UTILISATION OF NIST AS A CYBERSECURITY FRAMEWORK IN HIGHER
EDUCATION INSTITUTES DURING COVID-19

Research Document

by

Thomas Hughes

C00231519

APRIL 29, 2021

Supervisor: Christopher Staff

Table of Contents

Abstract.....	2
Introduction.....	3
Overview of Areas, Technologies or Topics researched	3
Sample Surveys/ Research	3
Research Survey.....	4
NIST CSF.....	4
NIST CSF AUDIT	7
COBIT.....	8
HEAnet.....	8
National Cyber Security Centre	9
National Cyber Security Strategy.....	9
EU Directives – NIS & ENISA.....	10
Cyberattacks on HEI’s	11
NUIG Galway	11
University of Sunderland	11
HSE 2021 attack	12
Cyberattack Responses.....	13
Summary and Conclusion	14
Glossary	15
References.....	16
Table of Figures	17

Abstract

The research document for this project takes both a quantitative and qualitative data based on the efficacy of Irish Higher Education Institutes' cyber and IT security, particularly during the COVID-19 period of 2019 – 2021. This will be analysed and compared in this research document by a series of past cyber attacks within this period, analysing the attacks and the responses, and how the institutes moved forwards. The research document will also look at standards used outside of Higher Education, using the NIST CS framework as a metric.

Introduction

As long as we remain online, we remain at risk. This is the fundamental rule of cybersecurity. This means every service you interact with has (hopefully) some sort of security in place to defend itself from cyberattacks. Higher Education Institutes (HEI's) have online services, but due to the COVID-19 pandemic, practically all institutes were forced to use online learning full-time for a period. This put a huge strain on these services, and forced most unprepared institutes to adapt their services to accommodate this change. This was a great move for them, but had every IT security professional concerned; *how protected were these HEI's?*

Writing now in late 2021, most universities and institutes have found the benefit of blended learning – a mix of online and in-person.

Overview of Areas, Technologies or Topics researched

In this section, the areas listed will be all forms of technology researched deemed relevant to the project. Each point of interest is explored, each being noted for its relevance to the project.

Sample Surveys/ Research

As a part of the research project, a cybersecurity survey was to be implemented. The results compiled from multiple HEI's will not only give a strong overall view of how listed HEI's perform in this metric as a standard, but also allows a scoring system to show how they competed against each other. Firstly, however, existing surveys were researched, based on cybersecurity questionnaires, mainly sent to companies. The varying range of relevance of these surveys/ questionnaires gives a broader scope to work with when designing the Cybersecurity Readiness Questionnaire.

Cyber guidelines? Regulations? How is data being protected? These are questions that will be considered when creating this survey.

Following the research conducted on these mentioned surveys, a sizeable amount of info is compiled and sought as a framework for the Cybersecurity Readiness survey. This will help structure the planned NIST survey's questions and provide inspiration for the types of questions to be asked.

Research Survey

Following the list of surveys and questionnaires researched, a survey is to be created to assess the cyber readiness of a Higher Education Institute. This is the first draft created, with questions to consider and notes on each.

Cybersecurity Survey Questions

Below are 22* cybersecurity and IT security-related questions designed to assess your HEI's state of preparedness in these areas.

1. Does your institute have a chief information security officer (CISO) or equivalent?
2. [How do you prioritize your institute's most critical/valuable informational assets? (Avoid "sensitive" data, data protection) Types of assets e.g. business info, IPs, contracts w/ suppliers (explanation of what's meant) *]
3. Do you have a form of asset management in place for your institute's assets? E.g. PCs, laptops, switches, servers (add list of terminology to explain)
4. What tools do you use to monitor your assets? 3rd party? In-house? *
5. Do you periodically review user activity on your network?
6. Monitor to access points?
7. Do you have a cyber security risk assessment for your institute?
8. What types of cybersecurity policies do you have in place currently? (provide list)
9. How often do you have cybersecurity training for students and staff?
- Every 12 months? 6 months? Longer?
10. Are staff & students required to sign an acceptable use agreement at hire?
Staff only, stud only, both, neither
11. How to ensure your students/ staff complete this training?
- Mandatory training day? Signed completion form? Other _____
12. Do you have any online resources to spread cyber awareness? To students or staff? If yes, please explain
13. On a scale of 1 – 5, how prepared do you feel in a cybersecurity attack? List – ransomware, DDoS, email phishing etc. * 9 (separate in to individual q's for each attack) (how well to prevent? Or how well to recover?)
14. On a scale of 1 – 5, where 1 is not prepared and 5 is very prepared, how prepared do you feel to prevent a DDoS attack?
15. On a scale of 1 – 5, how prepared do you feel to prevent a ransomware attack?
16. On a scale of 1 – 5, how prepared do you feel to recover from a ransomware attack?
17. On a scale of 1 – 5, how confident are you about your incident response to a cyber attack? Do you have a response plan in place? Incident + response? Incident for each scenario in Q 10.
18. Do you have a response team or an individual?
19. A) How often do you review your mitigation techniques proactively?
 - i) - not at all
 - ii) - Only after attack?
 - iii) – Only after significant changes to environment E.G. move to online learning?
- B) How often do you review your mitigation techniques reactively?

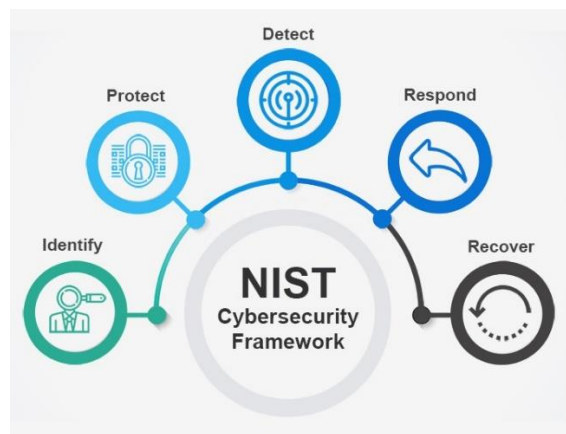
[FIG 1]

NIST CSF

As assumed by the title, NIST will be the framework focussed on in this project. The research of this framework will help me in understand how it works, and more importantly how to use it. Being able to utilise this framework, understand its particular benefits, while also

comparing it to other frameworks and their benefits is crucial to getting to use it in the most effective possible way.

“Created through collaboration between industry and government, the voluntary Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.” – (NIST, 2018)



[FIG 2]

(Cyberwatching.eu, 2020)

The NIST framework has proven to be highly valuable for different organizations, used officially by commercial companies such as JP Morgan, Microsoft, Boeing and Intel to name a few. The framework has been given the green light by the US government also, confirming roughly 20 states use the framework. Given the reputation of such a dynamic security framework, it chosen it as a standard to compare the quality of frameworks and practices that HEI’s had in place.

The draw of NIST for managers and board members is the top-down approach and its direct simplicity. NIST is broken down into five core functions, known as the Framework Core:

- Identify
- Protect
- Detect
- Respond
- Recover

These five functions are the spine of the whole framework, that are followed by other elements under these core titles. They allow users, typically management, in quickly identifying and controlling their cyber security risk within their organisation and allowing management of that risk.

As mentioned by The **Identify Function** is defining users, people, data, and systems for managing bodies in a way that allows them to understand the context of their business in these actors terms. Identifying these actors allows those managing to recognize their roles as they support essential functions, as well as the risks linked and needs required to meet them.

For example, the framework mentioned by (NIST, 2018) gives a few definitions:

- Physical and software assets are identified as part of asset management
- Business environment is identified, role in supply chain & in critical infrastructure is noted
- Cybersecurity policies identified to define governance, legal & regulatory requirements for organisations capabilities
- Asset vulnerabilities are identified, risk response is practiced
- Risk management for risk tolerance is identified

The **Protect Function** highlights the appropriate protection techniques to be utilised in infrastructure. This revolves around control and access allowed within organisations. This includes;

- Awareness and training
- Access control for physical and remote devices
- Organisation with maintenance
- Procedures and policies for third parties

The **Detect Function** is the detection of anomalies and security events. This includes:

- Maintaining detection software
- Monitoring anomalies and events
- Impact of events are understood and improved upon

The **Respond Function** is the procedures and actions taken to respond to an attack both before and after. This is combined with the ability to understand an impact and respond to it appropriately. This includes;

- Comms with stakeholders for impact analysis and transparency
- Mitigation techniques to plan for future events
- Understanding effective response techniques
- Defined personnel for a response event

The **Recover Function** is the final function, the appropriate steps to return to business-as-usual status, and how to retain that.

The NIST framework is broken into different standards, each standard being more suitable for a different organisational environment.

NIST CSF AUDIT

A NIST Cyber Security Framework Audit is the measurement used to determine if an organisation

The benefit of a CSF Audit is hugely beneficial to the project. Being able to gauge how successful a HEI’s fundamental organization and security is will give a very valuable insight into how prepared a HEI may be during a particularly vulnerable time – particularly during the switch to online/ hybrid learning during the COVID-19 lockdown period.

ComplianceForge Products	NIST 800-171	ISO 27002	NIST 800-53	NIST CSF	PCI DSS	23 NYCRR 500	EU GDPR
Cybersecurity & Data Protection Program (CDPP) or Digital Security Program (DSP)	252.204-7008 252.204-7012 NIST 800-171 (multiple CUI & NFO controls)	5.1.1 [multiple sections]	PM-1 [multiple sections]	ID.GV-1 [multiple sections]	12.1 [multiple sections]	500.03	Art 5 Art 25 Art 32
Supply Chain Risk Management (SCRM)	252.204-7008 252.204-7012 NIST 800-171 NFO PS-7	15.1.1	PS-7 SA-4	ID.SC-1	12.8	500.11	Art 32
Cybersecurity Risk Management Program (RMP)	252.204-7008 252.204-7012 NIST 800-171 NFO RA-1	11.1.4	PM-9 RA-1	ID.GV-4 ID.RM-1 ID.TM-2 ID.RM-3	12.2	500.09	Art 5 Art 25 Art 32 Art 35
Cybersecurity Risk Assessment Template (CRA)	252.204-7008 252.204-7012 NIST 800-171 3.11.1	11.1.4	RA-3	ID.RA-5	12.2	500.09	Art 35
Vulnerability & Patch Management Program (VPMP)	252.204-7008 252.204-7012 NIST 800-171 3.11.2	12.6.1	SI-2 SI-3(2)	ID.RA-1 PR.IP-12	6.6	500.05	Art 5 Art 25 Art 32
Integrated Incident Response Program (IIRP)	252.204-7008 252.204-7009 252.204-7010 252.204-7012 NIST 800-171 3.6.1	16.1.1	IR-1	PR.IP-9	12.5.3 12.10	500.16	Sec 1 (49)
Security & Privacy By Design (SPBD)	252.204-7008 252.204-7012 NIST 800-171 NFO SA-3	N/A	Privacy Section SA-3	N/A	N/A	N/A	Art 5 Art 25 Art 32
System Security Plan (SSP) & POA&M	252.204-7008 252.204-7012 NIST 800-171 3.12.4	N/A	PL-2	N/A	N/A	N/A	Art 32
Cybersecurity Standardized Operating Procedures (CSOP)	252.204-7008 252.204-7012 NIST 800-171 (multiple CUI & NFO controls)	12.1.1 [multiple sections]	PL-7 [multiple sections]	PR.IP-5 [multiple sections]	N/A	500.02	Art 5 Art 25 Art 32
Continuity of Operations Plan (COOP)	252.204-7008 252.204-7012 NIST 800-171 3.6.1	17.1.2	CP-1 CP-2 IR-4(3) PM-8	RC.RP-1	N/A	N/A	Art 32
Secure Baseline Configurations (SBC)	252.204-7008 252.204-7012 NIST 800-171 3.4.1	14.1.1	CM-2 CM-6 SA-8	PR.IP-1 PR.IP-3	1.1 1.1.1 2.2-2.2.4	N/A	Art 32
Information Assurance Program (IAP)	252.204-7008 252.204-7012 NIST 800-171 NFO CA-1	14.2.8	CA-1 PM-10			N/A	Art 5 Art 25 Art 32 Art 35

[FIG 3]

The (**Compliance Forge, 2022**) product table shown above may seem like a self-endorsing piece of data at first, but on further inspection, it gives us valuable comparison data for different NIST frameworks & corresponding frameworks used for IT security compliance.

As noted by the table, the NIST 800-53 framework (using their metric of inclusion in their security documentation) compares strongest for inclusion of features. It is worth knowing that this may be the most in-depth framework to use for the research project, but that doesn't necessarily mean it will suit the type of organisation (an HEI) as different frameworks are better-suited for covering different organisational structures – as is the purpose of these differing frameworks. As is the nature of exploring the cybersecurity capabilities and preparedness of HEIs, the NIST CSF will be a focus for the project.

COBIT

<https://www.isaca.org/resources/cobit>

COBIT (Control Objectives for Information and Related Technology) is an internationally recognized tool for modern businesses, and had been recommended to include in my research by both academic and IT professionals. COBIT is a tool that aids different organisations in “in regulatory compliance, risk management and aligning IT strategy with organisational goals.” (**IT Governance, 2021**)

A few points brought to attention when researching was the push for accountability and governance within organisations in an effort of cybersecurity. While this is a point of interest promoted by NIST, there are tools such as COBIT that highlight this importance with their sole responsibility of focussing on it. Having looked at recent cyber-attacks, an underlying issue raised was the frequency at which accountability and governance was not clearly defined. COBIT, particularly COBIT 5, the newest edition, notes that governance is needed to ensure there is accountability after these events, for the sake of protecting the organisation effectively next time.

HEAnet

The HEAnet provides internet and IT services for Ireland's higher education sector. Services such as eduroam and FileSender are highly valuable resources used by students and academic staff. In addition to these, the HEAnet has involvement in research by providing publications and workshops that detail their yearly improvements and studies. This, coupled with the transparency of the group makes it a reliable service for HEI's. The HEAnet has a large

responsibility providing a 24/7 service to the HEIs that use it, as student services are reliant on this.

This source will be relevant to the project as they have close connection to the target of the topic – higher education institutes. While it may be unfeasible to access more precise details of each of the HEI’s via this source, the transparency of the group’s resources and information will be useful for assessing the

[National Cyber Security Centre](#)

The National Cyber Security Centre (NCSC) was effort to provide guidance for Irish organisations with cybersecurity infrastructure while researching cyber information.

“Established in 2011 and is the government’s operational unit for network and information security. The role of the NCSC is to lead in the management of major cyber security incidents, provide guidance and advice to citizens and businesses, and manage cyber security related risks to key services. – **(Government of Ireland, 2021)**

Found on the official NCSC website, the NCSC currently has a list of cybersecurity documents that act as guides for various groups of organisations, both public and private i.e. Baseline Standards is mainly of note as it covers the guidance for Public Sector bodies for when securing their networks. This applies directly to the type of organisations worked with on this project, so having an awareness of the NCSC is important when considering certain choices made by HEIs.

[National Cyber Security Strategy](#)

Officially a follow-up to the initial security strategy published in late 2019, as mentioned by **(Government of Ireland, 2021)**, the National Cyber Security Strategy is a broader and more comprehensive document than the last one, and is informed by the operational experience gained by the National Cyber Security Centre (NCSC) from 2015 to 2019, and from ongoing national and international engagements in the area.

The main takes from the strategy is the development of the previously mentioned NCSC by was the Gardai’s involvement in performing risk assessments for all established organizations related. A theme of requiring guidance from top-down is a common one when it comes to HEIs in Ireland.

A main criticism from leaders (**Biddulph, A., 2022**) in the field was the lack of mention of budget in the strategy. This leads those that follow this strategy in an uncomfortable situation of uncertainty regarding funding from the government. Funding, as explored within this document and later in this project, is a crucial component to the security of every organization that is usually harder to come by, particularly in Higher Education Institutes.

The relevancy of the NCSS to the project is that the target audience to be contacted will presumably be following this strategy, and this will need to be considered when taking into account the answers received from these HEIs.

EU Directives – NIS & ENISA

Ireland has its own policies and legislation for governing cyber security. It also abides by the collective legislation that is imposed by the EU. “The EU Network and Information Systems Directive 2016/1148 was signed into Irish law on 18 September 2018 by way of S.I. No. 360 of 2018.” – (**Government of Ireland, 2021**)

The NIS Directive’s overall aim is to ensure a standard level of network and cybersecurity within the EU, particularly essential infrastructure. As Ireland classifies HEIs as essential services, this would be applicable for my target audience.

The NIS Directive, set up by the European Union Agency For Cybersecurity (ENISA) established 3 main sections;

1. All nations in the EU must be to a level of cyber security. This is verified by cyber audits and exercise,
2. Collaboration between nations
3. Supervision of national critical sectors

(ENISA, 2021)

The relevancy of the NIS Directive to the project is that the target audience to be contacted will presumably be following this strategy, and this will need to be considered when taking into account the answers received from these HEIs.

Cyberattacks on HEI's

These following examples are the recorded attacks, and probably the most valuable cases for me to record for this project. This shows both how attacks were performed, how the HEI responded to the incident, and the details of how other HEI's have responded. They also bring light to the current state of online preparedness for HEI's.

NUIG Galway

(Nuigalway.ie. 2021)

During the academic year of 2021, National University of Ireland, Galway was hit with a significant cyber-attack. The attack was detected and believed to have affected the university's online services. The IT response team's initial action was to shut down all online services, however due to the COVID 19 pandemic, most college services are dependent on the retention of their online capabilities. Once the shutdown occurred, many students and staff were stuck without any facilities, causing major concerns and disruptions to learning. There were also raised concerns on the integrity of user data, and if it had been stolen during the attack, to which NUIG denied.

On a later inspection of the NUIG response to this, the official NUIG site has many resources regarding cyber awareness, including phishing, spam emails, open-desk policies, password protection, online data storage, and further. This particular response seems like the right thing to do in my opinion, as it acknowledges the attack, and to some degree takes accountability, and shows initiative to improve in any way possible. It shows an effort of cyber awareness that is greatly needed in Irish HEI's.

The attack is not only significant for IT Carlow, but for all HEI's. The attack boils up questions that inspired this whole research topic: what sort of defence do the Irish HEI's have in place for cyberattacks? What supports do these institutes have in place, be it third-party or government-issued? Is there enough work being done to provide assistance to increase resistance to cyber-attacks?

University of Sunderland

(BBC News. 2021)

Mid-October of 2021 saw University of Sunderland having been on the receiving end of a cyber-attack. It was reported that all IT services, online and telephone services were offline. The university had remained offline for a couple of weeks. The university had remained quiet

about the attack, and unlike NUIG, had little to no acknowledgment of the attack. Noticeably the site also had no cyber awareness in response to this.

These particular cyberattacks are relevant for a multitude of reasons. The attacks highlight the universal issue of cybersecurity and defending against cyberattacks and how these are not exclusive issues to Irish HEI's. Not only are these attacks common, but they can prove successful, even against larger institutes which presumably have a higher priority and spending on IT Security and cybersecurity features.

HSE 2021 attack

<https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf>

The Health Service Executive (HSE) is the public healthcare provider in Ireland. It is publicly funded and services the public for health and social care in the country. Being the main public health service, the HSE would have access to hundreds of thousands, even millions of people's sensitive data e.g. health conditions, income bracket, medical history, addresses. This has made the HSE a big target for criminal hacking groups, having proven vulnerable by the 2021 cyberattack, in which the HSE's system was breached.

The HSE cyberattack official report mentions that the initial stages of the attack were caused by a successful phishing attempt of a Microsoft Excel file downloaded onto an HSE legacy machine. This phishing attempt allowed a ransomware attack to be carried out.

In light of the reports of this attack, many recommendations were taken on-board by the HSE. This includes:

- New roles were set up in the HSE – Chief Technology and Transformation Officer and CISO (Chief Information and Security Officer)
- Developed investment plan for transforming legacy IT systems to include security
- A security crisis plan to be managed and developed
- Allowing ethical hackers to test their systems

As previously mentioned, a huge underlying issue for many of these established organisations, particularly in Ireland, is the lacking of both cybersecurity prioritization and governance in the management board. Hindsight is always 20/20 with these attacks, however it is clear that the HSE fell victim to an attack by being unprepared, under resourced and underestimating the severity of the gaps in its security, both on a technological level and a managerial level.

The relevance to link to my research project is that of its identity as a public sector organisation, how it has been managed with IT security in mind, and the use of training and awareness brought to staff to fill these gaps in security. Another notable point is the fact that this attack took place during the COVID-19 period, and how it greatly affected the processes of the organisation significantly due to this.

Cyberattack Responses

As mentioned in the NUIG case, many HEI's have been looking over their shoulders after seeing these previous attacks occur. This prompts my research even further – are HEI's anticipating attacks in the most effective manor?

As an example, Trinity College Dublin (TCD) updated their website to reflect their concerns of the NUIG attack (found at <https://www.tcd.ie/itservices/security/>). This site includes a page dedicated IT security for staff and students by providing an informative video that includes basic IT security terms, and also gives a list of tips that should be practiced by the users in order to protect their data & devices.

These sorts of resources are important to provide for the users on your system, and this can be described best with the old saying “a chain is only as strong as its weakest link”. According to Verizon Data Breach Report 2021, “phishing was involved in 36% of breaches” – (Tessian, 2022). Having such a high success rate means a larger focus on the efficacy of further phishing attacks, and the effort and planning in these attacks become greater. As secure as your systems may be, there is still a reason why phishing emails are still so common today.

This goes back to the aforementioned saying – if your users are your weakest link, your organisation is still very much open to attack.

Another important goal these sorts of resources achieve is the way users think about IT and their data, especially HEI's. It's common to find varying levels of IT literacy in both students and staff, meaning it can be challenging to highlight the importance of users and their data, as well as being able to enforce security policies and practices. For many users, technology and computer use can be daunting, especially for older mature students and users that may not have been literate with technology to begin with. Student-friendly resources can help open up this relationship for users, and begin cultivating a mindset that allows these users to be more

confident with tech as opposed to being intimidated by it. The same way universities may have student resources designed to help them get used to college life, there should be a positive environment surrounding the IT side of this. Allowing your user base to ask questions and explore is an important step to helping them be conscious of the real dangers of data protection as a concept. This both enables your organisation to become more secure, strengthening your “weakest links” and allows you to focus your security efforts elsewhere.

Summary and Conclusion

The document highlights the various technologies covered, and the relevant research will be implemented in the final project. Namely the research on the surveys will be implemented in the Cybersecurity Readiness Survey, having analysed the templates, and understanding the content of the IT-based surveys, these will be used to develop and test these to provide the greatest chance to acquire the most valuable information. These surveys along with the extended research of NIST CSF to perform a successful NIST-based audit on a specific HEI will prove to be valuable assets for this project.

Glossary

COBIT	Control Objectives for Information and Related Technology. An international tool used by organisations, with a focus on accountability and governance.
COVID-19	Also recognized as Coronavirus, having caused a global pandemic. Majority of the world's countries remained in prolonged lockdown periods, where human contact was limited.
ENISA	European Union Agency for Cybersecurity is an agency designated to the EU to help provide cyber policy and improve cybersecurity awareness among the EU nations.
EU	European Union. The group of countries in alliance politically & economically found mainly within the continent of Europe.
HEAnet	Ireland's national education network researcher and provider. Operates as a centralised network e-infrastructure for many universities in Ireland, keeping students and staff connected across the nation.
HEI	Higher Education Institute. HEIs are colleges/ institutes of technology/ universities that provide tertiary-level education.
HSE	Health Service Executive. Ireland's national public health service provider.
IT	Information Technology. The use of systems for storing, retrieving, and sending information.
NCSC	National Cybersecurity Centre. Established by the Irish Government to provide resources & guidance for public & private organisations to enable and ensure a level of cybersecurity to protect themselves.
NCSS	National Cybersecurity Strategy. A strategy proposed by the NCSC in efforts to improve the cybersecurity of Irish organisations.
NIS	EU Network and Information Security directive is the first EU-wide legislation. Used to protect EU members on a cybersecurity level by keeping them at a equal standard.
NIST	National Institute of Standards and Technology. NIST provides standards for different aspects of tech, including their highly praised cybersecurity standard.
NUIG	National University of Ireland, Galway. The leading Higher Education Institute in Galway, one of the leading universities in the country, located in the west of Ireland.

References

1. **BBC News, 2021.** *Sunderland University cyber-attack fix date unknown.* [online] Available at: <<https://www.bbc.com/news/uk-england-tyne-58925807>> [Accessed 25 November 2021].
2. **Biddulph, A., 2022.** *Analysis of the Irish National Cyber Security Strategy - BH Consulting.* [online] BH Consulting. Available at: <<https://bhconsulting.ie/analysis-of-the-irish-national-cyber-security-strategy/>> [Accessed 16 April 2022].
3. **Compliance Forge, 2022.** *NIST SP 800-53 R5 Moderate Policies, Standards & Procedures.* [image] Available at: <<https://www.complianceforge.com/solutions/nist-sp-800-53-r5-moderate>> [Accessed 16 April 2022]. **[FIG 2]**
4. **Cyberwatching, 2020.** *NIST Cybersecurity Framework.* [online] Cyberwatching. Available at: <<https://cyberwatching.eu/nist-cybersecurity-framework>> [Accessed 9 December 2021]. **[FIG 2]**
5. **ENISA, 2021.** [online] Enisa.europa.eu. Available at: <<https://www.enisa.europa.eu/topics/nis-directive>> [Accessed 29 April 2022].
6. **Government of Ireland, 2021.** *Cyber Security.* [online] Gov.ie. Available at: <<https://www.gov.ie/en/policy-information/5e101b-network-and-information-security-cyber-security/#national-cyber-security-strategy>> [Accessed 21 October 2021]. (NCSS)
7. **Government of Ireland, 2021.** *Cyber Security.* [online] Gov.ie. Available at: <<https://www.gov.ie/en/policy-information/5e101b-network-and-information-security-cyber-security/#national-cyber-security-strategy>> [Accessed 21 October 2021]. (NCSC)
8. **Government of Ireland, 2021.** *Cyber Security.* [online] Gov.ie. Available at: <<https://www.gov.ie/en/policy-information/5e101b-network-and-information-security-cyber-security/#national-cyber-security-strategy>> [Accessed 21 October 2021]. (EU Directives)
9. **IT Governance, 2021.** *COBIT 5 framework for the governance of enterprise IT.* [online] Itgovernance.co.uk. Available at: <<https://www.itgovernance.co.uk/cobit>> [Accessed 27 March 2022].
10. **NCSC, 2019.** *National Cyber Security Strategy 2019-2024.* 2nd ed. [ebook] NCSC. Available at: <https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf> [Accessed 16 April 2022].
11. **NIST, 2018.** *Getting Started.* [online] NIST. Available at: <<https://www.nist.gov/cyberframework/getting-started>> [Accessed 25 November 2021].
12. **Nuigalway.ie, 2021.** *Blackbaud-Incident - NUI Galway.* [online] Available at: <<https://www.nuigalway.ie/alumni-friends/updateyourdetails/dataprivacystatement/blackbaud-incident/#>> [Accessed 25 November 2021].
13. **PricewaterhouseCoopers, 2022.** *Conti cyber attack on the HSE.* [online] PricewaterhouseCoopers. Available at: <<https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf>> [Accessed 20 April 2022].

- 14. Tessian, 2022.** *Phishing Statistics (Updated 2022) - 50+ Important Phishing Stats - Tessian.* [online] Tessian. Available at: <<https://www.tessian.com/blog/phishing-statistics-2020/>> [Accessed 7 April 2022].

Table of Figures

[FIG 1] Cybersecurity Readiness Survey draft

[FIG 2] Cyberwatching “NIST Cybersecurity Framework”

[FIG 3] Compliance Forge Product Table