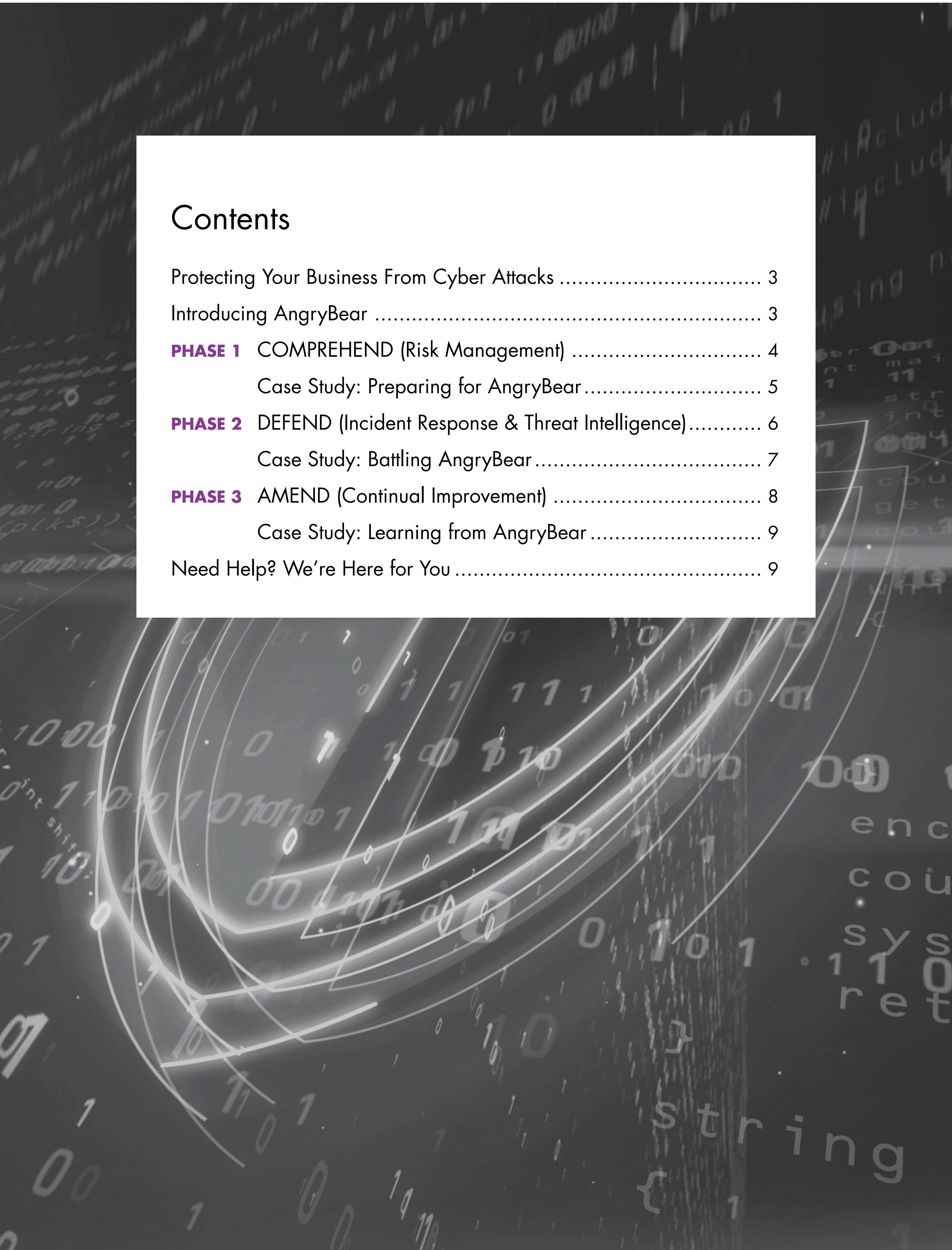
A FREE FRAMEWORK: IMPLEMENTING MEASURES TO COUNTER CYBER TERRORISM IN BUSINESS

www.dig8ital.com

dig8ital



Contents

Protecting Your Business From Cyber Attacks

As we've increasingly seen in recent years – Petya, WannaCry, SolarWinds – organizations are increasingly at risk of cyber attack from the world's advanced persistent threat groups (APTs), otherwise known as cyber espionage groups or, colloquially, hackers.

Your company is a part of the global digital supply chain, and that means you must be prepared to defend yourself against acts of cyber attack, espionage and terrorism, whether you're the target or become collateral in an attack against one of your vendors.

In this guide, we will offer you a checklist to follow that breaks down measures to mitigate the risks and potential damage of such attacks, with guidance on how to implement each step.

Introducing AngryBear

To help contextualise this framework, we'll use a fictional APT: AngryBear.

AngryBear is a suspected Russian hacker group associated with the FSB. Its members typically target telecommunications organizations in Europe and the Middle East, with two primary objectives: espionage (through the use of spyware) and disruptions to service (through the use of ransomware).

Their common tactics include:

Wide-net phishing of telecommunications employees.

Social engineering of key industry individuals (i.e. IT managers).

Attacking with malware via malicious and highly infectious smartphone apps.

Spoofing of enticing PDFs riddled with further malware – spyware or ransomware.

PHASE
1

COMPREHEND (Risk Management)

The COMPREHEND phase is all about preparation. Here you will learn to evaluate your business, account for its every component and put in place the pieces required to respond quickly to real-life cyber attacks.

Objective	Y/N?
Collected - and have put in place the steps to maintain – a list of all company assets. Additionally, have put in place plans to monitor this list to ensure accuracy over time.	
Cyber attacks can come from almost anywhere, and every component of the business is a risk. It's vital to learn what your business owns, where it is stored, who owns it and how it is protected.	
Instructed cyber teams to research top potential threats to your business, and the toolkits commonly used by such threat groups.	
Know thy enemy – it's one of the first steps in any battle. If you understand which current APTs are a risk to your company, and the tools they commonly use, you can better prepare to defend against them. To learn more, click here.	
Conducted an audit on the current security posture of the organization, taking into consideration threat intelligence, monitoring levels, software patch levels, and so forth. Additionally, have plans to conduct this audit bi-anually.	
Know yourself - that's the second step. It's hard to know where to go if you don't know where you are, so this audit is designed to present an 'as-is' state of the business with regards to security.	
From this audit, have identified security priorities and top concerns, and have assessed which risks are acceptable to the business and which are not.	
A list of risk priorities will help you understand what to fix first as we proceed. Not all risk is made equal, so there may be some areas that don't require immediate attention. To understand this step, you will need a risk appetite. To learn more, click here.	
Created security thresholds to benchmark against. These thresholds monitor for changes in security status of critical assets.	
Monitoring for anomalies is a powerful strategy in the fight against cyber crime. But to know what an anomaly looks like, you need to know what 'normal' looks like - which is what this step helps you understand.	
Have established business continuity plans, using ISOs 22301 and 22313 for guidance on the topic.	
Business continuity plans exist to help keep your business operational during a calamity (not just cyber attack), and the process of creating them will show you holes in your organizational agility that must be filled. To learn more, click here.	
Put together an incident response team.	
A well-trained incident response team can reduce the cost of a cyber breach by as much as €330,500 (IBM). This team will be multi disciplined (IT, HR, PR, legal), with the goal of containing breaches, investigating the cause and coordinating a response. To learn more, click here.	

Continued over page.

PHASE
1

COMPREHEND (Risk Management) Cont...

Objective	Y/N?
Built a ‘quick-win’ book of solutions that can be used quickly to safeguard an infected asset, and monitor for future attacks.	
This book is in PDF form and is highly summarised – to be used fast. Such quick-wins may include ‘disable Office Macros’, ‘find out what other apps are connected to the infected app (warn those teams)’, ‘raise a ticket with defence teams’, ‘check for the most recent back-up’, and so on.	
Built awareness of cyber security among staff through training and workshops.	
Your people are your biggest vulnerability, and always will be. But you can mitigate the likelihood someone will make an innocent, yet costly, error with good training. Consider also peer-to-peer training as a means to help staff feel they aren’t being talked down to.	
Reviewed how all of the above information is gathered and shared among stakeholders, and have plans to conduct this review annually or bi-annually (which is preferred).	
Any missing information at this phase of the framework could lead to gaps in security later. So, it’s vital to know how you are going to gather this information and keep it updated as your business - and the threat landscape – evolves over time.	
Total:	

CASE STUDY

Preparing for AngryBear

In this case study we assume we are a mid-sized telecommunications company in Germany. We have a few hundred staff and offices across multiple cities.

Our security team has identified AngryBear as a potential threat after it was revealed to have hacked a competing organization. By studying the group, we learn their common attack methods and objectives as outlined earlier in this book.

Looking into our own security posture and 'as-is' status, we see we have both hardware and software at risk – old hardware and out-of-date software both need updated. We're also using a basic firewall approach, as opposed to a more modern philosophy such as ZeroTrust.

Staff training at our company is also deemed deficient, and workshops are planned to build awareness of cyber security issues. These workshops will be hosted by security teams, not higher-ups, so they feel less condescending – peers helping peers, not bosses telling subordinates what to do.

PHASE
2

DEFEND (Incident Response and Threat Intelligence)

As we move into phase two, you have already laid a strong foundation of knowledge – knowledge about your company, its risks and its threats. In the DEFEND phase, you will identify what to do if an attack is detected!

ALERT: CYBER WARFARE ATTACK DETECTED

Objective	Y/N?
Upon detection of threat, incident response team (IRT) immediately safeguarded the infected asset using an array of quick wins from the quick-win playbook described above.	
These quick wins will not be enough to completely resolve the issue, but taking fast steps now could help prevent the infection from spreading and causing more harm. That is why we created the book in the previous step.	
Communicated the detected breach and safeguard measures taken thus far to the IRT member associated with analysis of cyber events.	
With strong action taken quickly, the next step is to analyze and understand the threat. The IRT member(s) associated with this step must be made fully aware of everything that has happened, and what is known, up to this point.	
Validated the accuracy, scalability and source of the cyber attack event.	
As a part of the analysis, the IRT must learn where the attack came from, how quickly it has been able to/is able to scale, and how accurate current intelligence is with regards to its harm.	
Leveraged threat intelligence to assess the effectiveness of controls against the specific type of attack.	
This step answers a key question: Did the control measures work? And how effective are controls generally against this type of attack?	
Results of the analysis have been shared with the IRT member(s) associated with taking further action, and they have been instructed on the action required.	
Quick wins alone are not enough - more measures will be required. It is vital that there is streamlined, fast communication between members of the IRT so that the right actions can be taken at the right time.	
Operational teams have begun implementing security measures to fix identified issues.	
At this point, Ops teams can be mobilized to implement the security measures identified earlier, looking to stem the harm of any symptoms currently being felt due to the attack.	
Strategic teams have begun implementing security measures to fix identified cause(s) of the issue.	
As Ops works to close the wounds, Strategic teams must look to the root cause to ensure that the same kind of attack cannot happen again.	
Total:	

CASE STUDY

Battling AngryBear

Despite measures being taken, they weren't quick enough – AngryBear has struck our telecommunications company. Ransomware has been injected into the customer service platform and it locked us out of this vital network. AngryBear is demanding payment for the release of the system.

Our incident response team immediately isolates the system from any other and checks for its most recent back-up – two of our quick wins.

Analysis experts look into the attack to determine the best course of action, and to identify the extent of the attack (i.e. is there more unidentified malware in the system?).

Three actions steps are agreed upon and communicated to the appropriate teams:

1. The infected system is deleted and replaced with its most recent backup, thus avoiding the need to pay attackers to regain access.
2. The hunt is on for other unidentified malware, and action is to be taken as required.
3. The hunt is also on for the source of the ransomware – who downloaded it and when?

PHASE
3

AMEND (Continual Improvement)

The DEFEND phase will last as long as it needs to in order to cycle through the entire process of reacting to, analyzing and then controlling a cyber breach. When the dust settles and the threat is secure, you can move into the AMEND phase – which is all about lessons learned, and how to do better.

Objective	Y/N?
Organized and held workshops with key stakeholders (i.e. those involved, as well as other relevant personnel) on lessons learned.	
By putting everyone involved (as well as other key people, such as board members or directors) in the same room to talk about lessons learned, you can create valuable feedback to improve your company's response to future events.	
(If workshops can't be held for any reason) Conducted online surveys and one-on-one interviews to gather the same data from involved team members.	
Workshops can't always be held, but you still need this vital information. Using online forms or one-on-one interviews can get you similar, if not the same, information. You could also use a hybrid approach to gather thoughts individually then discuss them as a group.	
Passed on all feedback to relevant team members and, if recommendations were made for improvement, put in place a plan to make said improvements.	
Talk requires action. Ensure that all feedback is passed on to the relevant people and that they fully understand the what, when, why, who and how of these improvements.	
Ensured that all improvements are factored into future audits so they can be taken into account in future.	
You must understand how to measure these improvements, and have an agreed process to monitor those KPIs over the coming months. Then, when you come to repeat this framework in future, the auditing step also factors them in so success can be fully measured.	
Total:	

CASE STUDY

Learning from AngryBear

Now that the ransomware has been dealt with and services are returning to normal, we can begin to look into what went wrong. So what did we learn and what are we doing?

The IRT responded quickly and effectively, but we identified that the ransomware snuck through a manager who was socially engineered to download an app – which then spread additional phishing materials to a subordinate, who downloaded a malicious link.

As a part of the feedback process, relevant team members were praised where they did a good job and their work was publicly recognised.

A key area of improvement has been noted: Training workshops may have been missed on certain staff members, or were ineffective. We need to identify why this person was missed and talk about how training can be improved. Additional feedback surveys will be required – perhaps asking staff their thoughts on the training, and areas they don't feel confident.

Need Help? We're Here for You

With the company's reputation on the line, as well the safety of its staff and customers – and not to mention regulators constantly monitoring for malpractice – it's totally understandable if the idea of preparing for and responding to a cyber attack seems like a lot to handle alone.

That's where dig8ital comes in.

We're experts in cyber security and mitigating the risks of cyber terrorism. With vast experience in the evolving threat landscape backed by real client results and a team of qualified professionals, we know what it takes to prepare for and defend against real-life cyber attack situations.

To gain a better understanding of this cyber warfare framework and how it works, or to speak with someone about your organization's unique concerns,

contact us for a free maturity consultation.

W: dig8ital.com
E: contact@dig8ital.com

dig8ital