EBOOK

What to Look for When Evaluating Your Cybersecurity Strategy

http://www.trumbull.tech

Table of Contents

CHAPTER ONE:

A Growing Threat to Cybersecurity

Cybersecurity is a serious issue, and probably more serious right now than ever before . It is estimated that by 2021, the cost of combating and dealing with cybercriminals could be around $6 trillion, and profits from cybercrime itself could outstrip those of the illegal drugs trade.

Scary statistics, certainly, but there is no need to panic. Instead, you and your organization need to be taking a methodical and considered approach to cybercrime, and putting in place the measures necessary to your precious data safe from would-be thieves and exploiters.

This is the ethos behind our e-book. Read on to discover more about how to develop and evaluate your cybersecurity strategy.

"It is estimated that by 2021, the cost of combating and dealing with cybercriminals could be around $6 trillion …"

CHAPTER TWO:

What Kind of Data Needs to Be Protected?

Modern businesses rely on data. They need this data to provide the right kinds of products and services to customers, as well as to optimize their position in the market. This translates to vast amounts of data that needs to be managed, utilized, and – of course – protected.

But, businesses need to be savvy about this last aspect – protection. After all, treating all of this data as one homogeneous whole is going to make real protection difficult to achieve. Only by examining the data, by understanding which parts of this data are most under threat or are most valuable, both to the organization itself and to cybercriminals, can truly effective data protection be implemented.

In short, all data needs to be protected to some extent, but protection needs to be tiered. The most stringent protections need to be put in place for the most valuable – and most at-risk – datasets.

What Is the Most Valuable Data?

This is the data that needs to be protected with the most robust measures. But, how do you decide which data is the most valuable? Consider these factors:

- Which datasets does your organization rely upon for its daily operations? In other words, this is the data that your organization simply cannot function without.

- Which datasets are subject to local and federal law? As an organization operating in the United States, you are legally required to adopt minimum standards of protection for the data you retain and use. Different state jurisdictions apply different laws.

- Which datasets are considered sensitive? This refers to any data that could give away critical information regarding your customers, partners, employees, the company itself, or any other entity.

- Which datasets do you think could be the most vulnerable? We'll explore this in further detail in the Analyzing Vulnerabilities section.

Answering these questions will give you an idea of which of your datasets are in most need of protection.

Who Has Access to This Vital Data, and Why?

In order to do their jobs properly, your employees need to be able to access and use the data that your organization stores. But do all of your employees need to access this? The answer is, definitely not.

Start by considering the reasons why you are storing this data in the first place. You are not keeping hold of it for a rainy day, hopeful that it will be useful in the future. Instead, you are using it to fuel your long and short-term strategies, to support your day-to-day operations, and to optimize your position in the market. This means the data needs to be accessible.

"...all data needs to be protected to some extent, but protection needs to be tiered."

Start by thinking about the different roles that each of your team members carries out within your organization. Think about how these team members need to use data – particularly, the critical data outlined above.

This is where tiered access plays a huge role. Digital platforms are already incredibly important to the operations of businesses across a variety of industries, and they make it easy to achieve close integration between stored data and the processes that rely on it. They also allow businesses to set access tiers and privileges to safeguard this data from unauthorized access.

When Are These Datasets Accessed?

It is important to remember that access requirements change over time, so accessibility needs to change, too. Go back to those crucial datasets you identified – now that you have considered who needs to access them, think about when.

It could be that operatives only need to use this information at certain periods each year. Or, it could be that access to the datasets is project-specific and needs to be managed accordingly. Each individual who accesses this data is a potential weak spot, so precautions should be taken to limit data access to when it is most necessary.

Keeping on top of projects and data requirements is critical to risk mitigation. Deploy project management software to outline the data requirements of each project. Then feed this information back to project platforms so tiered access can be implemented. This can be a serious drain on resources, but it is necessary to ensure that only the appropriate users have access to datasets at the appropriate times.

CHAPTER THREE:

Analyzing Vulnerabilities

We have already discussed how certain datasets may be more vulnerable than others within your organization. This is why it is so important to analyze the vulnerabilities that could be affecting data security in your business.

Let's take a look at some possible examples.

Possible Vulnerabilities Within Your Business' Data Strategy

- Contractor employees or third-party partners – Contractors and third-party partners may not have received the requisite training in data security, so they may not be aware of their duties and responsibilities as users and custodians of data.

- Recent hires or employees still undergoing training – Recent hires also may display the same weaknesses as those from third-party organizations. This is why data security needs to be an inherent part of training from an early stage.

- Long-term employees – In truth, no employees can be considered invulnerable. Long-term employees display different weaknesses to recent hires and contractors, in that they may be so set in their ways that their actions become second nature. This may lead them to make errors in judgment. Mitigate this by implementing ongoing training and appraisals throughout an employee's time with your company.

- Shared passwords and access credentials – In an ideal world, each employee has their own access credentials and only ever uses these. Unfortunately, we do not live in an ideal world, and these credentials do get shared from time to time. Educating employees on the dangers of doing this, and even operating biometric access protocols if resources allow, prevent this danger.

- Employee emails and devices – Remote work policies are undoubtedly beneficial to businesses, but they also expose your organization to potential weaknesses. Develop a safe use policy for remote devices and vet each device before it is used. Extend this practice to employee emails and deploy robust anti-virus and anti-malware protections.

- Payment gateways – Payment gateways are interfaces across which money changes hands. As such, they can be potential weak points. Make sure that your data security tools cover these weak points.

- Other pieces of software and hardware – Every piece of software and hardware must be assessed for potential vulnerabilities. We will be taking a look at the differences between cultural and technical vulnerabilities, and how to tackle both, in the next section.

Cultural and Technical Vulnerabilities

Vulnerabilities can be divided into two main groups – the cultural and the physical. The way you tackle these vulnerabilities depends on the category.

Tackling Cultural Vulnerabilities

Cultural vulnerabilities – as the name suggests – are rooted in the culture of your organization. These may include these examples:

- Team members sharing passwords and devices, or leaving themselves logged into systems when not working

- Team members transmitting sensitive information via unsecured networks

- Team members talking about client or customer data with unauthorized personnel

These above examples, among others, are not usually malicious. Instead, they come from a lax approach to data security. Rather than simply disciplining members of staff after specific breaches, a cultural overhaul is required.

This may take the following forms:

- Outlining an organizational charter regarding data security – This way, data security rules become a part of your company identity, and your entire team takes ownership of them.

- Refocusing training to cover cyber- and data security in greater detail – Often, improved education is key. We'll be exploring this further in the Educating Employees on Security Protocols section.

- Modifying the hiring process to reinforce cybersecurity threats from day one – Bringing in personnel with a strong track record on digital safety, and who have already been made aware of security measures and protocols during the onboarding and hiring process, is critical to fostering a more positive culture in the workplace.

"Products in development may be delayed, extending their time to market and further impacting profit."

Cultural shifts represent a fundamental necessity for companies looking to strengthen their security protocols. But, it cannot work all by itself. Instead, it must be supported by other initiatives.

Tackling Technical Vulnerabilities

Technical vulnerabilities are found in elements like hardware pieces or software platforms. These elements are critical to the day-to-day operation of your organization, but it can also leave the door open for potential cyber attackers or other threats.

You can tackle these risks in a number of ways:

- Assess the strategic impact – Take the knowledge you gained from Part 2 of this e-book and from the identifying vulnerabilities section of Part 3. Then, think about your risk tolerance level, i.e., how much risk can your business handle in each area? As there is no such thing as zero-risk, and as all risk mitigation measures carry a business impact of their own, you need to make sure that your strategies are cost-effective, each and every time. Don't implement risk mitigation strategies that are going to run your business into the ground in terms of financial and resource cost. If you think this might be the case, a different approach may be required.

- Conduct a vulnerability scan – Software such as Content Management Systems and Customer Relationship Management platforms will often either feature in-built scanning technology or support plug-ins that achieve this aim.

- Discuss vulnerability reports – Take the data from your vulnerability scan and apply this to research data taken from your own team. Discuss these reports and use them to inform your future strategies.

- Adopt a proactive approach to updates and replacements – Are the software and hardware your organization is using definitely the best and most robust on the market? Make sure you are constantly updating and upgrading your hardware and software architecture to make sure it is performing as it should.

- Work with a managed services provider – It can be difficult to manage security updates and vulnerabilities by yourself. Working with a managed service provider often represents a more cost-efficient and more effective way of achieving long-term security.

Tackling these technical vulnerabilities, alongside cultural ones, as part of a broader, unified strategy, is critical to achieving the security your business needs.

What Should Your Data Breach Plan Look Like?

You cannot achieve anything in business without a plan and a strategy. This is particularly true when it comes to defending against, and responding to, data breaches.

Of course, the best way to combat cyberattacks is to stop them from happening at all – a wholly preventative model. Unfortunately, in practice, this does not always work. And, even if it does work, you need a contingency plan in place to respond in the event of a data breach.

So, let's consider this data breach plan. But, before we get into the plan in detail, let's think about what you should be doing immediately after a data breach.

What Should You Do First After a Data Breach?

The critical hours following a data breach can be stressful and scary, and this can result in panic. In turn, this can lead to you forgetting all about your carefully and meticulously designed plan.

Here is how you respond to the breach in the right way and avoid losing your head at this critical time.

There Is No Need to Panic

Panicking will get you nowhere, and it may make it more difficult to execute a careful and considered response. Keep calm and make sure your thoughts and actions are practical, rather than haphazard. Think about what you can do to put this right.

There Is No Need to Pay Any Requested Ransom

Ransomware is a serious issue in the modern business landscape. It has been reported that in 2019, ransomware attacks were the most common form of malware attack, a fact that will make uncomfortable reading for business owners. Despite this, do not be tempted to pay the ransom and release your data. Doing so may help the attacker get away undetected, leaving others under threat. There is also no guarantee that the attacker will release your data simply because you paid up.

You Need a Team You Can Rely On

This team is the group that will orchestrate and execute your response and recovery plan. It goes without saying that you need your best personnel to carry out this task – a team you can really trust. Decide who this team will be ahead of time, and make sure each member of the team understands their respective roles and duties. You could run some practice drills to make sure everyone understands what to do.

"It has been reported that in 2019, ransomware attacks were the most common form of malware attack ..."
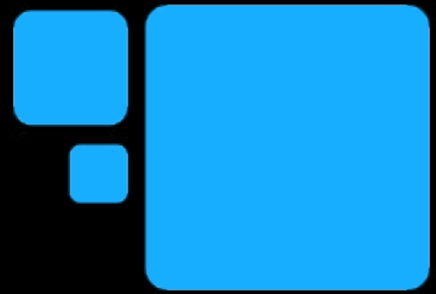
Don't Delay Switching to Backups

It is difficult to attach an exact dollar cost to business downtime, but it is safe to say that this is something you want to avoid. With this in mind, make sure you have backup servers in place, and switch to those servers immediately, as you attempt to secure maximum business continuity for your clients and customers.

Start With Containment

Malware and other malicious pieces of software can spread rapidly. Deploy firewalls and redundant server and storage architecture to contain the damage and harm caused by the breach. Separate physical storage devices from the network if necessary, limiting the damage done.

Analyze and Understand the Breach

It may not always be immediately evident just how much damage has occurred. This is why your team needs to become investigators, analyzing the extent of the data that has been compromised, and trying to get to grips with how this happened in the first place.

Keep a Record of Everything

As your team investigates the breach and tries to gain a firm understanding of the issues that lay behind it, it is important to keep a documentary record of the process. You will need this documentary evidence later on, as you make insurance claims, press charges against criminals, and seek to shore up your defenses against such attacks in the future.

Be Transparent

You may not want to do so – and it may feel awkward and nerve-wracking – but you have to inform your customers, clients, partners, and any other stakeholders about the breach. It is your duty to do so, and withholding any information may be considered bad practice at best, and may be illegal at worst. You need to show that you are responsible and serious about safety – this means being fully transparent in your efforts to put things right and coming clean about what has happened.

Try to Learn From the Experience

A data breach is a severely negative experience. However, that does not mean that you can't learn something from the experience and apply this knowledge to your strategies in the future. Use the information you gain from this troubled time for your business, go over the records you have kept regarding how the breach occurred and was dealt with, and make your organization more robust and better protected than ever before.

What Should You Include in Your Data Breach Response Plan?

We've already taken a look at some of the steps you can implement in the aftermath of an attack. However, it is important to make sure that your employees are not simply springing blindly into action in this event. This is why you need to draw up a solid plan beforehand, and make sure your employees are well aware of all its aspects.

"It is important to make sure that your employees are not simply springing blindly into action in this event."

Here's what you need to include in your plan:

- Education for staff members on sensitive data – All of your team members need to be aware of what constitutes sensitive data. Make sure that your whole team is knowledgeable on this, and is aware of what needs to be protected.

- The personnel that makes up your response team – Having a crack response team is very important indeed, so make sure to select your response team ahead of time. Remember to select a diverse array of skill sets so you can cover all bases, and make sure you have your best personnel on the job. You will also need to appoint leaders and deputy leaders within this team structure.

- The priorities for your response team – In the heat of the moment, it may be difficult for your team to decide on the best course of action for your business. Make sure that your plan includes the tasks and actions that your response team needs to prioritize on their way to dealing with the breach.

- Personal responsibilities across the whole team – Following a breach, it is not just the response team that leaps into action while all other personnel sits around doing nothing. Even if a team member is not selected to join the elite response unit, they still have their own duties and responsibilities that they must take care of, probably within their own area of expertise at the company. Make sure everyone is aware of this.

- Lines of communication – Communication is critical. Internal lines of communication dictate how you will coordinate your response to the breach, while external lines of communication are critical to you remaining transparent and cooperative with stakeholders and authorities. Decide which lines of communication will be primary and how these will be managed.

- External assistance – You may need to call upon external assistance to help you manage the breach. This external assistance may come in the form of a managed service provider or another body. Decide realistically on your capacity for handling the breach yourself, and the threshold for calling in external assistance.

- Legal backups – In the majority of cases, a data breach is a crime. As such, the issue is a legal one, and you will need legal advice and representation. Plan ahead for where this legal support will come from to make sure your organization is completely prepared.

- Drill schedules – It is no good to simply put your plan in place and then hope for the best. You need to drill and practice this plan, as well as reappraise it and possibly modify it over time. Decide on a schedule for drilling and assessing, and be sure to stick to it in order to achieve maximum preparedness for your organization.

Educating Employees on Security Protocols

Education is the constant that runs through all aspects of your data security strategy. Without education, your team is doomed to make the same mistakes time and time again, without learning or developing. Without the proper approach to education, it's going to be difficult to understand the threats that are out there and how to work against them.

We've already touched on education briefly earlier in this e-book. But here we're going to look a little more closely at this aspect of defense, starting with what to include in this process of education.

What Should You Include in Your Data Security Education Programs?

- The importance of data security within company culture – It is not usually enough simply to tell your teams about how important data security is. Instead, you need to demonstrate the position of data and cybersecurity within the overarching culture of your organization. This will make it more likely that your team members will take active ownership of your data security issues, and consider them to be of extremely high importance.

- The legal responsibility of data protection – Company culture is one thing, but the law is something else entirely. All of us have been brought up with an understanding of what the law is and what it means. Make sure that your staff understands how, why, and in what way data security is a legal issue.

- The practical elements of engaging in good data security behavior – This is something you will need to tailor to different members of staff, or at least members of staff on different teams. Each team has its own duties and, therefore, its own actions that need to be carried out in accordance with data security best practices. Make sure these practical elements are made clear to your entire team.

- The warning signs to look out for – You and your teams need to be proactive and look out for warning signs of impending attacks or other suspicious activity. Of course, for this to be possible, your teams must first know what these warning signs look like. Build this into your education strategy.

- The process of response – What happens in the worst-case scenario? How do you respond to a data breach? You and your team need to know this, so make sure that this is covered in detail within education and training procedures.

"Without the proper approach to education, it's going to be difficult to understand the threats that are out there and how to work against them."

How Should You Provide Education and Training?

It can be difficult to really engage your team members and make sure that they take ownership of the problems, even when the potential stakes are so high. So, how can you better engage your team members and build a solid defense against cybercrime?

- Mimic the real thing – We have discussed drills already in this e-book, but it is important to mention this again as this method of training is so crucial to getting the message out there. It also demonstrates exactly what these teams will need to do in the event of a real breach.

- Bring in upper management – Everyone needs to be onboard during training, and this really means everyone. If upper management is involved and has thrown its collective support fully behind the training program, this underlines how critical it really is to the business as a whole.

- Start the process early – During the onboarding stage, the new hire is learning a great deal of new information. While you may not want to add to this, it is crucial to find room to educate on cybersecurity issues from the very beginning of their career with your organization. This will help the new hire to foster and nurture the right habits, every step of the way.

- Assess and appraise – You have set your training schedule, you have outlined its content, and your team members are learning a lot about how to keep the business safe. Now what? Well, you need to assess and appraise how the program is working, as well as examine how much your team is learning in a practical sense. Remember: Your education program can always be improved.

- Appoint a representative in each team – Ensure that each department and each team is able to pull together by appointing a training representative in each unit. They will be able to offer ongoing support and assistance across the whole organization.

- Provide rewards and incentives – Take a positive approach to cybersecurity, although the subject itself is a negative one. Reinforce good behaviors with rewards and incentives, and focus on helping your team to develop and grow their skill and capability levels.

Final Thoughts:
Working With the Right Partner
to Fill the Gaps

We hope you have enjoyed our guide to developing and evaluating a robust
cybersecurity strategy. We also hope you have learned some critical
information to take back and apply to your own business.

Cybercrime is a costly affair, costing organizations an average of $3.92
million per instance in 2019. This is why we developed this guide as a way of
helping your business to avoid such disastrous costs.

"Without the proper approach to education, it's going to be difficult to understand the threats that are out there and how to work against them."

However, we also know that it's not easy for businesses to fill all of the potential security gaps themselves, and to guarantee their own safety. This is why it is often a good idea to work with a third-party managed services provider to make your defenses extra robust.

Get in touch with our team today to learn more about how this could help you and your business, and to discover the difference an MSP can make to your security strategy.

Trumbull Tech LLC
205 S Hoover Blvd #413
Tampa, Florida 33609

http://www.trumbull.tech
8137716625