Vigilance & Diligence: How to Protect Your Company From Cybersecurity Threats

Michelle Drolet
CEO, Towerwall

towerwall

Vigilance & Diligence: How to Protect Your Company from Cybersecurity Threats

Table of Contents

About the Author

As the CEO of a woman-owned cybersecurity company and one of Towerwall's resident information security experts, Michelle Drolet assists organizations through the process to help them protect critical data by the evaluation, establishment, education and enforcement of sound information security, network security and data security programs and practices.

Foreword

Staying abreast of the latest cybersecurity trends can be a tricky challenge for modern businesses, but it's absolutely vital if you want to safeguard your data. Plugging vulnerabilities, keeping your cloud secure, and avoiding phishing scams and ransomware attacks requires diligence, user awareness, and vigilance.

The cybersecurity market is growing fast and will be worth almost $250 billion by 2023, according to Markets and Markets. As ever stricter data directives and compliance mandates come into play and cyber-attacks grow ever more sophisticated, companies need to be aware of what direction the wind is blowing to ensure best practices are followed.

A simple set of static plans isn't enough, you need a fluid strategy capable of reacting to the latest trends, but also proactively guarding against future threats.

What may seem like a gargantuan task becomes more manageable when it's broken down into achievable tasks, which is precisely what this eBook sets out to do.

You can drastically reduce the risk to your business by assessing vulnerabilities, delineating responsibilities, testing your defenses, and acting swiftly to bolster them when needed.

There's plenty of low-hanging fruit in your pursuit of security and all too often it's a simple lack of common sense and a failure to adhere to basic principles that leads to major disasters like the spread of the Emotet Trojan this year.

Taming cybersecurity threats requires a deep understanding of the landscape and a commitment to invest in the lifeblood of your business: your staff.

Just as employees add enormous value, they also increase your potential attack surface. A strong cybersecurity strategy goes beyond software and hardware to educate and empower.

Each chapter in this eBook tackles a different topic related to cybersecurity and offers clear, practical advice on staying ahead of the threat and protecting your company.

You can dip straight in with a subject that interests you, or work through the chapters in order. You'll find an overview of each trend followed by reasoned advice, seasoned by my 25-years of experience in cybersecurity, and ready for you to act upon.

Achieving a strong cybersecurity posture is an ongoing battle that requires continuous research, but we're here to help you in your journey to a more secure future.

Michelle Drolet
CEO, Towerwall

10 Best Practices to Secure your Organization

The risk of a data breach is ever present and can prove disastrous for any business. It's vital to guard against cyber-attacks, but also to establish solid plans to ensure you react to any breach in the right way.

It has never been easier for cybercriminals to infect your business with malware or ransomware. A vast array of malware tools can be bought on the dark web, complete with helpdesks for hackers, so the barrier to entry is low. Most hackers will sit on your network for days, weeks, or even months, gathering intelligence to infiltrate your systems and then try to exfiltrate data undetected. While prevention is better than cure, it's not always possible. The smart move is to take what action you can to guard against intrusion, but also to employ intelligent real-time defenses, and to craft detailed action plans and procedures to handle any incidents that do arise. These best practices will help you reduce the risk of a data breach occurring in the first place, but also reduce the impact and damage if the worst does happen.

1. Establish a risk baseline

The first step in securing your organization is to determine what level of risk you are willing to tolerate. Every business is different. You must assess your data and workflows to find out what the key risks are that would damage your business, and plan to address them in order based on the threat that each one poses. It's unlikely you'll be able to cover every base, so to extract maximum value from your resources, make sure you understand where your baseline is and apply a triage approach.

2. Capture a complete picture of your network

From printers to security cameras to smartphones, the number of exploitable endpoints on your system is growing all the time. It's vital that you have a complete inventory of devices, including small devices and sensors that fit into the Internet of Things category. Your ability to protect your network depends upon you having a clear, fully mapped picture of it.

3. Build a user awareness program

It's easy to focus on the technology and tools that promise to bolster your security efforts, but the simple truth is that people are usually the weakest link in your defenses. People click on links they shouldn't, they respond to increasingly sophisticated phishing attacks, and they unwittingly invite malware onto your network. It's crucial that you train your staff to spot security risks and teach them how to respond appropriately. Put a proper security awareness training program in place and test your employees regularly to ensure that it's working.

4. Assess and patch vulnerabilities

Many data breaches occur because of a simple failure to address known vulnerabilities. Organizations can be alarmingly slow to update software and patch issues, even after alerts are sent out. Make sure you have a stringent update policy in place and consider employing a tool that can flag your

existing vulnerabilities.

5. Do root cause analysis

If an incident or a breach does occur, then treat it as a learning opportunity. You may assume that ticking all the boxes will keep your data safe, but new attack vectors are uncovered every day. A root cause analysis will enable you to identify the heart of your problem and remediate.

6. Implement real-time automated protection

Wherever possible you want to employ real-time tools that can scan for issues and resolve them automatically. Sometimes security teams are struggling with a backlog, so identifying a threat isn't enough, because there's a lag between the alert and the fix. Consider the role machine learning can play and think about user behavior analytics and other strategies for uncovering possible risks.

7. Craft an incident response plan

You can restrict damage, reduce recovery time and limit the associated costs by putting a robust incident response plan in place. A good plan lays out every detail of an effective response, making it clear who is responsible and what needs to happen every step of the way. Break it down, so you have a playbook for data breaches, denial of service attacks and ransomware attacks. Run drills to ensure that your plan is effective. These plans and exercises are also great to show regulators that you're taking your responsibilities seriously.

8. Fully utilize your existing security technology

It may be tempting to splurge on the latest security tools, but it takes some expertise to leverage security software effectively. Start by assessing the technology you currently have in place and make sure that you're getting maximum value from it. Sometimes a process tweak or reconfiguration allows you to secure much more with little or no cost.

9. Bake security into everything

Security should not be about firefighting; your CSO should be selling the importance of a strong information security strategy to every business unit in your organization. They need to be included as part of every conversation whether it's a new project, the development of a new application, or a new technology is being acquired.

10. Employ third-party risk management

It's highly likely that you work with third-parties and vendors and some of them will have access to your data. Your security efforts must go beyond internal strategies to consider third-party risk. Assess your partners, ensure they meet your standards, and test them on it – don't take their word for it.

Employing these best practices will help you to reduce the risk and potential impact of a data breach, but security is on ongoing process that requires constant attention. Your strategy should continually evolve for best results.

Five Steps to Create a Vulnerability Management Plan

Ensure you have the right strategy in place to detect advanced threats sooner rather than later.

While much of cybersecurity is focused on prevention, the simple fact is that many attacks are successful. Even a sophisticated, expensive security system is going to be breached from time to time. Smart attackers try to fly under the radar, biding their time and extracting maximum value or causing maximum carnage, sometimes over a period of months or even years.

The specter of a major data breach always looms large in the minds of InfoSec professionals, but it's not always external malware that's behind it; insider threats can be the toughest to uncover. There's also the risk of bad actors intent on causing reputational damage with peripheral attacks that are harder to interpret. The good news is that you can take steps to boost your chances of swift threat detection and effective action.

1. Understand your environment and risk tolerance

Security should start with a complete inventory, a fully mapped environment, and a deep understanding of what your business is all about and therefore what needs to be protected. It should be obvious that you need to know about all the potential endpoints and secure unmanaged devices, but the idea of risk tolerance is less straightforward.

The fact is you can't cover every angle, so discuss with key personnel and identify what is core to your organization. Once you've worked out what information must be tightly controlled, you can begin to put together the right tools and systems to safeguard it. With clear priorities you can also ensure that the most important areas get the highest level of monitoring.

2. Establish a baseline for normal behavior

Before you can spot the breadcrumbs that might lead you to a breach you need to have a clear and accurate picture of what normal operation looks like. Consider employing user behavior analytics, so that any suspicious activity on the part of employees is flagged for investigation. This can be very useful in rooting out, not just external attacks, but also insider threats and plain old mistakes that may cause exposure.

This is also an area where machine learning can play an increasingly important role. The difficulty is false positives, which can be disruptive and time consuming to identify and resolve. It's about supporting your experts, rather than replacing them.

3. Create a comprehensive incident response plan

Every business should build a robust incident response plan to restrict the damage that any attack

can wreak, reduce the recovery time to the absolute minimum, and limit the associated costs. Whether it's a cyber-attack, a natural disaster, or an ISP outage, you need to ensure that everyone knows what's required of them and set clear responsibilities to get back to normal operations as swiftly and painlessly as possible.

By establishing a clear set of instructions and procedures to follow in the event of different problems arising, you can guard against the kind of misguided reactive panic that makes a bad situation worse. If you've already completed the last two suggestions, then crafting an effective response plan should be straightforward.

4. Analyze and learn from incidents

The temptation to immediately slam the door shut when you detect a threat is understandable, but it should be resisted. You can pull a weed out, but if you don't get the roots it will return. Track the infection from the entry point to identify the back door. Every successful attack or breach is an opportunity to learn.

Root cause analysis is absolutely vital, not just to understand how and where your defenses failed, but also to learn how you can fine tune your security systems to ensure that a similar approach will not work in the future. Exposing an incident and tracking it will help you strengthen your defenses, improve your incident response plans, and identify weak spots in your systems or skill sets.

5. Create a skills map and test your team

The cybersecurity skills gap is well established and while you can mitigate to some extent by hiring a virtual CISO and engaging consultants, it's always going to be worth investing in and nurturing your existing talent. A proper, company-wide security awareness training program is essential, but you need to get more specific and dive deeper with your InfoSec staff.

There are lots of different certifications and security training courses out there, but you should stop and consider what's actually required. Everything we've looked at so far can be used to craft a skills map highlighting the skills you need to effectively protect your environment and guard against the kinds of threats that your company has had to face.

Think carefully about specialization, because you don't want two general practitioners when you could have a brain surgeon and an oncologist. Building an effective team requires specialized roles, but you may need to develop your own training techniques, using resources on the internet, that don't just teach, but also test that knowledge in a real-world, practical way.

Keep these prerequisites at the forefront of your mind as you develop a security strategy. Allow them to inform and feed each other, so your strategy evolves, and security grows stronger after you encounter incidents. This is the path to building a solid foundation for truly effective advanced threat detection.

For Cybersecurity to Succeed, You Must Embrace Penetration Testing

The specter of a data breach is ever present for companies today and it has led to an effort to tighten cybersecurity defenses, but how do you know if your efforts have been effective? Without regular penetration testing, you really don't

The threat of a cybercriminal gaining access to your network is a constant source of anxiety. Amid the high-profile data breaches, businesses and organizations of all sizes have been successfully targeted by hackers employing a wide range of different strategies. Too many companies have had to learn all about the potential cost of a data breach firsthand. The important thing to keep in mind is that all these companies had top-tier security measures and professionals, yet they were compromised.

Cybercrime is growing fast, it's becoming more sophisticated, and its proving very lucrative, which is attracting more criminals. Hackers can buy effective tools with support off the shelf in the dark web, so the barrier to entry is low. Little wonder Cybersecurity Ventures suggests that cyberattacks are the fastest growing crime and will cost the world $6 trillion a year by 2021.

There are many steps you can take to improve your security posture, but something that's often overlooked is the need to properly and regularly test the defenses that you've built. Breaches are inevitable, but you can learn from them and part of effectively preventing them in future is getting into the mindset of your attackers.

Where are we going wrong?

In the aftermath of a breach it's natural to ask, "Where did we go wrong?" Perhaps your business employed consultants, bought in a raft of security software, and took positive steps to shut down vulnerabilities. Maybe you trained your staff, invested in the latest tools, and employed a superstar CISO or brought in a virtual CISO. So, how did the hackers get in? Strong security is about more than committing resources, you have to cover all the angles, and that includes subjecting the defenses you've built to some serious scrutiny and stress testing.

"Penetration testing is very effective in finding and prioritizing the organization's true vulnerabilities," explains Amitai Ratzon, CEO of Pcysys. "But the way it is typically executed today is inefficient, expensive and infrequent. That is because up till lately there was no real alternative but to hire a Penetration Testing services firm to come in."

Many organizations, even very large companies, conduct annual penetration testing. That means once a year they subject their defenses to an internal and external attack designed to emulate a real hacker attack.

"How can you really be confident that your data is safe if you only test your defenses once a year?" asks Ratzon. "The risks and vulnerabilities are growing and changing all the time, and cybercriminals are determined and constantly evolving. There's a clear need for more frequent pentesting."

This concept is common sense. We've talked about the need to test effectiveness with your security awareness training or anti-phishing initiatives. You don't assume every employee gets it first time – you test them. We've talked about the benefit of real-time visibility and automated policy enforcement with regard to the IoT blind spot. These principles apply to pentesting as well.

Cybercriminals are persistent and determined and they will continue to hack away at your systems, often with automated tools, until they find a crack they can exploit.

Overcoming the barriers to continuous risk validation

It's not just the frequency that's creating problems here. Hiring pentesting companies is very expensive. The skills shortage across cybersecurity suggests that's not going to change any time soon. You're also putting a lot of trust in the company you choose and its employees, because they have access to all of your assets and knowledge of all your weak spots.

What if you could automate your penetration testing, have a research firm assure the test is most current, and run it continuously? We could move from an annual penetration test to monthly, weekly, or even daily testing. Pentesting can help you understand where to prioritize your security efforts. Instead of having an endless list of vulnerabilities that you methodically patch, you can cut directly to where the greatest risk lies and deal with that first.

We come back to this triage concept frequently in discussing cybersecurity because it's not realistic to build a 100-percent secure system, you have to focus your efforts where they're likely to get the best return and that is exactly at the vector of the worst probable breach.By effectively emulating real attacks you can unveil the areas that require speedy remediation and squeeze maximum value from your security investments.

The benefits go beyond security

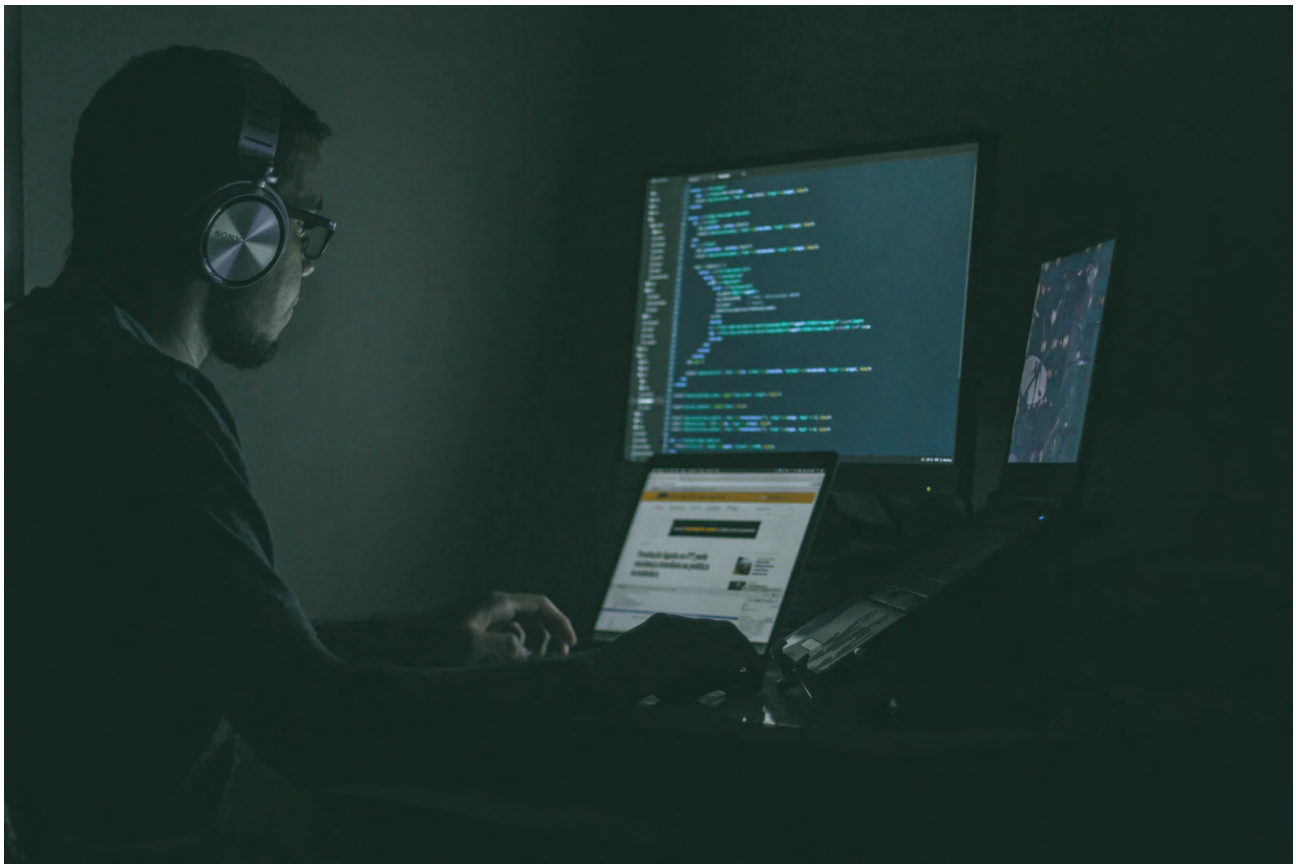
Automated penetration testing won't just enable you to improve your defenses against hackers, it can offer other important benefits. Firstly, consider the regulators. The GDPR is a journey rather than a destination, and regular testing and evaluation of your security efforts is an expected part of that journey. Annual penetration testing doesn't measure up to those requirements.

Secondly, if you turn to insurers to underwrite your cyber crime risk, then regular pentesting will allow you to provide tangible data that they can use to ensure your cover and your premiums are appropriate. This could be vital in the event that the worst does happen, because solid insurance can help you bounce back from a breach.

Cybercriminals are working continuously to break down defenses and uncover the path of least resistance. They are always probing for new ways onto our networks and they frequently sit there undetected. If we want to combat them effectively, we need to employ the same intelligent and determined approach.

Real-time protection and continuous assessment of our security strategies is needed, and automated

penetration testing is an important part of that. Pentesting is one of the greatest tools we have in the fight against cybercrime and it can deliver real, actionable insights, we must make more of it.



Cybersecurity penetration tests can save your company time and money in the long run.

How a Decentralized Cloud Model May Increase Security, Privacy

A new cloud model can support scalable applications while retaining safeguards of a decentralized, trust-minimized ecosystem.

Whether it's Amazon Web Services (AWS), Dropbox, Citrix, Microsoft or Google, all cloud storage vendors use the same basic principle -- they all sync and copy to a centralized cloud server cluster via the internet. Millions of users and their devices every second connect to these central cloud clusters to store and access files that are associated with their online accounts.

The cloud has been one of the greatest success stories of my generation, but a centralized server architecture has its shortcomings.

Loss of control

The dependence on remote, cloud-based infrastructure means taking on the risks of outsourcing everything. Even though most cloud computing platforms implement best of breed security practices, storing sensitive data and important files on servers belonging to external service providers presents its own set of risks. For example, most service providers take back-ups for off-line availability, creating multiple copies of files in various servers across geographies and leading to a broader threat surface.

And, though not the fault of the cloud provider, server misconfigurations leading to data leaks have become so common that they hardly make headlines anymore. One recent such example is the leak of a Dow Jones Watchlist Database, containing identities of government officials.

Privacy can also be a disadvantage for the cloud. Information on a public cloud can be legally and secretly accessed and exfiltrated by the provider, law enforcement agencies and in some cases foreign powers. The passing of the CLOUD Act last year obligates cloud providers like Amazon, Google and others to submit evidence to law enforcement should they be served a warrant -- even if the evidence is stored in another country or server.

Regulations like GDPR, HIPAA, SOX etc., may also become a hurdle because the actual compliance and management resides outside of your control.

Unexpected expenses

Adopting the cloud's pay-as-you-go model can be flexible and may seem to lower hardware costs. But if you calculate the overall price tag in the long run it can turn out to be expensive. Constant syncing of all users and their devices to the cloud can also lead to increased bandwidth overhead.

Vendor lock-in can also be another disadvantage for cloud computing. Switching between cloud platforms can lead to configuration complexities, additional costs and downtime. Compromises

made during the migration process can lead to security and privacy vulnerabilities.

Single point of failure

A recent configuration error on Google cloud servers disrupted services for up to four and a half hours and affected huge brands like Snapchat, Vimeo, Shopify, Discord, and Pokemon GO. Since cloud computing services are internet based, service outages can happen anytime and can occur for any reason and you have very little control over the whole situation. If a central controller is compromised, your data could be compromised as well.

Decentralizing the cloud

Although the existing cloud model is hugely successful, an upcoming generation of platforms plan to overcome some of the challenges cited above by focusing on decentralizing the cloud infrastructure with AI and blockchain. This new cloud model can support scalable applications while retaining safeguards of a decentralized, trust-minimized ecosystem.

According to a study by research firm IDC, by 2020, 45% of all data generated by IoT devices will be stored, processed, and analyzed at the edge of a network or close to it. The decentralized model uses the power of edge computing – moving processes and storage to the device at the edge of the network. The central server simply acts as a switchboard that enforces policies and creates point-to-point connections between data stored at endpoints or source locations. Edge computing enables endpoints to have their own cloud functionality of remote access, sharing, streaming, collaboration and file management.

“As opposed to centralized cloud storage that requires transferring and storing duplicated files over the internet to a central datacenter located miles away, a decentralized cloud or edge computing architecture addresses the inefficiency issues of uploading, downloading and syncing subsets of data to the limited storage capacity of cloud servers,” explains Thomas Ward, VP of Qnext, a developer of on-premises edge services.

In general, a decentralized architecture may provide additional security to cloud functionality. Files can be kept locally behind a firewall in select geographic locations and access controlled to protect the privacy and secret exfiltration from third parties, law enforcement and foreign powers. Data is not duplicated to third-party servers or secondary locations, which reduces the attack surface. Since files and storage are in an organization’s control, this also accelerates compliance with other regulations.

A decentralized cloud system runs on blockchain, making security of the network far stronger than what the current infrastructure offers because it provides security via compartmentalization. Even if attackers are able to access a block of data, they cannot infiltrate it as it is only a partial file. The architecture also splits files into small portions and replicates data across distributed file systems providing redundancy via multiple nodes. If a node is hacked or brought down, other nodes continue to function, presenting a failsafe that increases cloud stability.

This change in storage models won't happen overnight. But given the volume at which data is growing and the speed at which new devices (including IoT) are being added to networks, there will

be paradigm shift in cloud security strategies. And because the storage market is so large it's conceivable that we'll see more organizations following suit with a decentralized cloud computing approach.

"The decentralized cloud or edge computing architecture differentiates it from the centralized model used by file sync and share platforms. It improves the organization's security posture, allows access to all storage, ensures privacy, keeps the management of organizational files under organizational control, and leverages the organization's existing storage infrastructure," says Ward.

Whilst cloud-computing has it's benefits there are drawbacks to essentially outsourcing everything.

5 Ways to Improve your Cloud Security

As cloud adoption soars to new heights, security standards have failed to keep pace. Organizations need to start taking responsibility for their own cloud security and these five practical tips will help.

There's no doubt that widespread adoption of the cloud has enabled collaboration on a much greater scale, driving innovation and creativity. Distributed workforces can work harmoniously, IT departments can offload expensive hardware and maintenance costs, and organizations can benefit from the latest developments in software tools. But inevitably there's a catch.

Security has been forgotten in the excitement. Many companies have made the dangerous assumption that cloud service providers are responsible, a notion quickly dispelled in the event of a costly data breach. There are lots of different cloud security threats to worry about, so it's vital to craft a strong, comprehensive cloud security strategy.

To that end, here are five steps you can take today to improve your cloud security.

Establish full visibility

Organizations grow organically, acquiring and adopting new tools that must be integrated with legacy systems and building new relationships with different vendors and partners. A hybrid cloud environment, with data spread between on-premise servers and multiple external cloud services, is not unusual. Growing complexity can make it difficult to maintain a big picture view.

When 570 cybersecurity and IT professionals were asked about the biggest headaches in trying to protect cloud workloads, visibility into infrastructure security was the top answer at 43%, followed by compliance (38%), and setting consistent security policies (35%). You can't secure your cloud environment, no matter what it looks like, without having it fully mapped and establishing real-time visibility.

Train your employees

The clear majority of data breaches can be traced back to human error, whether it's misconfiguration, poor access control, a phishing attack, or a simple mistake. That's why proper security awareness training is so crucial. Arm your employees with the information and skills they need to reduce the risk of malware or unauthorized access and ensure that potential incidents are reported in a timely manner.

Ensuring that your staff have the skills they need to properly configure the tools they're using is just part of the equation. You'll also want to instill good security hygiene in them and set very clear policies about who is responsible and what the procedure is in the event of a potential incident. It's impossible to completely prevent errors, but the right response can make a world of difference.

Include security as early as possible

Part of the problem for anyone trying to secure the cloud is that they're typically retro-fitting security into a system that was designed with scant regard for it. Often those responsible for security struggle to convince under-pressure teams to change their processes. Barriers between departments can lead to resentment and resistance.

Bringing security into the fold and knocking down barriers is part of the shift towards DevSecOps, which allows for security to be designed in from the start of any project. This might be an ambitious goal, but the basic principle of including security as early as possible in any discussion is valid, whether it's about a new tool to adopt, software in development, or a change to your cloud architecture.

Continuously monitor

Being able to create a snapshot of your cloud and map precisely where your data is at any given moment is just a foundation, you also need to be continually vigilant for trouble. Data should be encrypted all the time, access should be tightly controlled, traffic should be monitored, and vulnerabilities need to be identified and remediated as swiftly as possible.

Continuously monitoring your network and feeding in fresh information about potential threats on an ongoing basis is vital. Make sure that suspicious behavior is flagged, so that you can uncover malicious insiders as well as unauthorized access. Build in clear audit trails for any data modification or deletion. The faster you find issues the better your chances of mitigating them.
.

Test regularly

Shifting data to the cloud does not shift your responsibility to your cloud provider, contrary to popular belief. If a data loss occurs your company will still be liable for regulatory fines, loss of public confidence, and all the rest of the associated fallout. That's why it is imperative that you perform due diligence on your partners and make sure they fully understand what compliance means for you.

The only way you can be sure that your defenses, both internal and external, are working properly is to test them. A regular testing program that encompasses everything from penetration testing to mock phishing attacks should be planned and implemented. Creating a feedback loop and stirring in emerging threats is the best way to ensure that your security systems are evolving fast enough. But don't forget to link tests to actionable remediation advice and empower your team to make the necessary changes. And let's not forget document, document, document.

There's a lot to dig into with cloud security and every organization's network looks different, but these guiding principles should stand you in good stead.

The vCISO: Is there one in your future?

When is the right time to rent yourself a CISO?

The enterprise is facing a dangerous combination of mounting cybersecurity threats of increasing subtlety -- and a widening gap in the skills required to identify and combat them. Having someone that knows how to lead the charge in identifying and analyzing threats, creating strategic security plans and ensuring compliance requires the right level of expertise.

The Information Systems Security Association spoke of a “missing generation” in information security, pointing to an estimated 300,000 to 1 million vacant cybersecurity jobs. To further complicate the labor shortfall, security professionals at enterprises understand they are in demand, and it is understood that employees will be receiving offers from other companies. According to a Ponemon study, senior security executives on average leave after 30 months on the job.

Almost three-quarters of respondents in a Ponemon report said their organizations do not have enough IT security staff. The fact is enterprises are looking to fill security positions. According to Burning Glass, a labor analytics firm, cybersecurity job postings grew 74% over a six-year period. But actually filling those positions is another story.

Finding the right person to drive enterprise security

According to Cisco's Annual Security Report, 91% of companies have an executive with direct responsibility for security, but only 29% of them have a Chief Information Security Officer. Businesses with a CISO in place recorded the highest levels of confidence in their security stance, both in terms of optimization and clarity.

Many organizations are asking other executives to step into the gap and they often lack the expertise required to outline a solid information security policy and drive it forward. Would you want a podiatrist filling in for a neurosurgeon?

For small to mid-sized businesses it may be difficult to justify the expense of a full-time CISO. Recruitment can also be a real challenge. How do you find the right fit for your business within your budget when you lack the internal experience to properly evaluate a candidate?

Enter the virtual CISO

For smaller businesses it simply doesn't make sense to invest in a full-time CISO when you can hire a virtual one and get the specialty skills you need to draw up a strategic overview and deliver the big picture. With a virtual CISO, no need to worry about benefits or monthly overhead.

Say you’re a larger enterprise. You're suffering from attrition and need someone to step in on an interim basis. You want some supervision and advice for a relatively green InfoSec manager, or you want to ensure that you only pay for what you actually need. Renting a CISO could be the answer.

Making the business case for a vCISO

There’s no set universal standard for hiring a vCISO. You can set up a retainer for a certain number of hours, you can hire someone on a project basis, and/or you can even buy a chunk of support hours and use them when you need them. It's a way of getting the cream of security talent without buying the whole cow.

Contracting a virtual CISO can be far most cost effective than hiring a full-timer. They can fill in where you need it the most, helping your CIO pull together your security policies, guidelines, and standards. That could entail anything from coming to grips with HIPAA or PCI compliance, to staying on top of vendor risk assessments.

A qualified vCISO is going to be fully up to speed on the latest best practices, they have experience dealing with a wide variety of scenarios, and they are well-positioned to train your internal security staff.

The normal annual contract rate for virtual CISOs is about 35-to-40 percent of what it costs to pay the normal industry salary for a full-time information security team to perform the same services, according to Bank Info Security.

Preventive security vs. post-incident cleanup

Many companies are being forced to spend an ever increasing proportion of their budget on cleaning up after incidents. A vCISO can be invaluable as a firefighter, but don't wait until a breach occurs; prevention is always better than cure.

Whether you're looking to get a snapshot of your security posture, fill a temporary gap, or you need a leader to roll out a company-wide InfoSec policy, the vCISO is a compelling value proposition. Until the new generation of security graduates matures, the vCISO may be your best shot at tempering security risks.

Don't Bite that Phishing Bait: Bet on these 5 Rules

Although bad actors have for years taken advantage of unpatched systems, countless software vulnerabilities and new devious forms of malware, their most preferred weapon of choice still remains the same.

When it comes to digital malfeasance, cyber criminals still use phishing as their trusted trick. While their motives haven't changed -- luring target victims to click highly legitimate-looking emails so they can steal keys to the castle – their attack methods have grown more targeted and sophisticated.

According to a recent FBI investigation, phishing scams cost American businesses half a billion dollars a year. More alarming evidence is seen in a public service announcement from the FBI issued earlier this year to spread awareness regarding the continued increase of "Business Email Compromise / Email Account Compromise," calling it a $12 billion scam.

Cyber security is only as strong as its weakest link – people

Even though businesses spend millions of dollars on cyber security solutions, sophisticated attacks such as phishing scams continue to thrive. The reason is simple. Cyber criminals are no longer hacking firewalls since all they need is a vulnerable employee. The fundamental reason why enterprise security fails to successfully battle advanced cyber-attacks is not for lack of competency but a lack of awareness training and policy-setting among employees.

a. Highly localized phishing scams

Phishing is all about deception and cyber baddies are evolving their methods to trick people in their sophisticated phishing scams. For example, moving away from their "infect them all" approach, phishers are turning to regionalized email attacks and location-based targeting. In their bid to customize phishing attacks and make their email scams more believable, cyber-criminals are becoming ever more crafty at imitating local brands and speech mannerisms, while not failing to use correct spelling and grammar like their predecessors had.

b. Phishers head to the cloud and other third-platform technologies

Attackers are reshaping traditional phishing techniques and targeting new vectors. As a result, a growing number of modern phishing scams are now distributed via social media portals, mobile apps or mobile browsers. Instant messaging (IM) applications are also being used to spread the attack to the victim's contact lists. Since users read and act upon real-time text notifications quicker than they read and act upon regular email, the attack proliferation happens faster. Moreover, with more businesses and users turning to cloud applications, attackers have begun launching more advanced cloud-phishing attacks. A highly sophisticated phishing campaign targeting Google's roughly 1 billion Gmail users worldwide is one such example.

Simple and effective ways to avoid the phishing bait

Even as organizations implement advanced security measures and also invest in cyber security awareness, both corporate and government environments need to do more to train employees. What makes phishing attacks really attractive is the opportunity to steal readily offered credentials or admin privileges directly from staff that allow attackers to gain further lateral movement in the targeted network.

Below are a few useful guidelines that will help safeguard you and your business from phishing attacks.

1. Make them familiar with the phishing hook

Phishing is one of the most effective means to get around security systems to steal sensitive data, usually in the form of a well-crafted email that imitates legitimate communications from trusted sources like your CEO, service provider, banks and even delivery companies. Recent phishing attacks that targeted Gmail and Office 365 managed to fool even savvy users. Encourage employees to join you in the battle by being able to recognize and hence sniff out the phishing scam. Always be on the lookout for red flags in any message received. Inspect every email message carefully, especially if it has any sense of urgency, or if it comes from an unknown sender outside your organization. An email may request an action that may seem highly unlikely, including an unsolicited offer. Spotting emails that have links to non-standard web page addresses is also a useful practice.

2. Be careful when typing URLs

The Anti-Phishing Working Group (APWG) issued its Phishing Activity Trends Report for Q1 2018 that reveals a significant rise in unique phishing webpages found early in 2018. Phishing attacks frequently come in the form of embedded malicious links in emails that appear to be coming from familiar sources. It may contain a video or an attractive photo to encourage the unsuspecting recipient to click on it, only to unknowingly download lethal malware. Sometimes the email may request login details with a link that appears to be your company website. It is easy to avoid such phishing traps by always typing the URL into the address bar of your browser. Make a strict rule to never click unreadable links in emails.

3. Think twice before you open attachments

Cyber baddies find email their favorite attack vector as it makes distributing malware payload cheap and easy. Malware authors craft convincing spam and phishing emails that often carry dangerous attachments. Sometimes such a payload might be covertly hidden in zip/rar archives, or in Office documents as macros. To infect a vulnerable user, the email often includes an executable file. Identifying suspicious attachments isn't too difficult, if one is prepared to be careful. Malicious attachments are often commonly hidden within zip archives to trick spam filters—they can be easily recognized by their common file extension, such as: .exe, .bat, .com, .cmd, .cpl, .js, .jse, .msi, .msp, .mst and even Windows PowerShell script extension .psc1. A vast majority of spam and phishing emails carry such malicious attachments. Even if you do not recognize the sender, it's strongly recommended to submit the email for further scrutiny if it has an attachment. According to industry reports, some of these attachments are able to slip through known cloud-based security systems.

Since enticing gullible employees to click links, open attachments and visit URLs is the most effective way of breaching corporate security, it is important to have deeper messaging security in place that automatically scans and discards suspicious attachments.

4. Flag suspicious emails to your security teams

If you are not sure about the content of an email you have received, then you should report it without a second thought. Seek further advisory from your company's IT security team. Many companies follow a good practice of having email support specifically for suspected phishing emails and they help validate if a reported email is legitimate or not. You may also consider filing complaints at the Federal Bureau of Investigation Internet Crime Complaint Center.

5. Don't just patch your systems, also patch your people

Awareness and education remain your best defence against evolving phishing campaigns. As crafty phishing attacks manage to penetrate security defenses, it is necessary to train employees, making them better aware of various phishing tactics used by cyber fraudsters. These email-borne threats have become an endemic scourge and have lethal potential to damage your company's reputation. While it is indispensable to keep systems and applications up-to-date with the latest patch and security updates, it is equally critical to keep users informed by running regular security awareness training or by investing in a phishing simulator application that can test users through automated attack simulations and actionable reporting metrics.

Phishing certainly poses a significant risk to your organization and its information. Knowing how to identify a phishing attack is obviously the most ideal defense. If you manage to avoid the bait, the attacker will have no choice but to move on to the next target.

Battling Ransomware Part I: How to Prevent a Ransomware Incident

Ransomware attacks can prove extremely disruptive and expensive to remedy. Prevention is better than cure and ransomware incidents are easily preventable with the right action.

A few high-profile ransomware incidents have spread awareness and many individuals and organizations acted to protect themselves, which may have diminished the success rate of ransomware and prompted attackers to employ other means. A Kaspersky report shows a 30 percent decline in ransomware encounters between April 2016 to March 2017 and April 2017 to March 2018.

However, ransomware attacks are still alarmingly common. There's no room for complacency here. Ransomware is not defeated as a threat, it's still evolving, with new strains emerging and changing all the time. Malwarebytes actually recorded a 28 percent rise in attacks on businesses in the first quarter of 2018.

Cybercriminals like the path of least resistance, so failing to guard against ransomware is like an invitation. Here's a step-by-step guide on how to prevent ransomware attacks from gaining traction on your network and causing real damage.

Step 1: Educate people

It's vital to have a well-designed security awareness training program in place. Employees are often responsible for unwittingly inviting ransomware in, usually by clicking on links in emails and messages that prompt ransomware downloads. While 78 percent of people successfully avoided clicking the link in a phishing attack test last year, according to Verizon's Data Breach report, 4 percent of people did click. Unfortunately, it only takes one to infect your network. Another issue is the fact that most people don't report suspected phishing campaigns, depriving security teams of valuable data.

What's required is a comprehensive training program that focusses on your most valuable business assets and stirs in the latest intelligence on ransomware threats. Arm your employees with the knowledge they need to spot danger and avoid it. Make sure they understand the importance of reporting, even when they don't click. Because the threat landscape is constantly evolving, your training program must evolve too.

Attendance and completion of training should be mandatory, but the only way you can really be sure that everything has sunk in is to test your employees. Conduct simulated phishing attacks and share the results. People who fail should be required to undertake further training and repeated failures may require disciplinary action. It's important that staff understand they have some responsibility in your prevention efforts – guarding against ransomware is not just a job for your IT department.

Step 2: Deploy security software

There are many different software tools that can help enormously in detecting, blocking, and dealing with ransomware and other forms of malware. Deploy a next generation firewall, antivirus software, real-time network scanning, next gen endpoint protection, anti-phishing and URL filters. But bear in mind that identifying and installing solid security software is not enough, it also has to be properly configured and kept up to date.

Ensure you have the right skillset on your team to leverage the software you buy. Improperly configured software is a major route in for attackers and can also bury your security team in false positives. You may also consider restricting unauthorized software with application controls.

The so-called shadow IT issue, where business units install apps they want without IT department oversight, can cause serious weaknesses in your defenses. Where restriction isn't viable, you need to adjust your strategy accordingly and establish real-time visibility into people, devices, and systems on your network. Behavioral analytics can also be enormously helpful in quickly detecting anomalies that might indicate an attack.

Step 3: Verify and test backups

If you have a proper, regular backup system in place, then you never need to pay a ransom to recover your files. There are lots of backup solutions on the market, both software and hardware based. For maximum security of your most precious business data, you might consider both. Make sure you fully map what would be required to get your business operating again in the event of a massive data loss and ensure everything is backed up. Without proper backups, ransomware attacks can lead to catastrophic downtime that threatens the business.

Your ability to recover also depends on the backup being easily accessible. Make sure you have a set procedure that's clear and easy to follow, and make sure you test it. Try recovering backups and verifying their integrity to identify any problems in your backup system before you really need it. A Datto report found that 96 percent of managed service providers with a reliable backup and recovery system were able to recover from ransomware attacks.

Step 4: Test and tweak

We've already touched on this, but it's crucial to your prevention efforts, so it bears repeating. You should have an incidence response plan, we suggest building out a "playbook" for each scenario, like ransomware. This will help with testing every system and every procedure that you've put in place and make sure that it works as expected. Can your strategy cope with a mock ransomware attack? If not, you need to go back and analyze any failure, then make changes and test again until it works successfully.

While you can build a solid foundation to guard against ransomware, there's no completion point where you're done. Ransomware is evolving all the time. Cybercriminals are always developing new techniques to gain entry to your network. Your training, software, backups, and general strategy must continue to evolve and grow over time if you expect to continue to nullify the threat of ransomware.

While prevention is a serious and potentially expensive undertaking, it pales in comparison to the devastating impact of a successful ransomware attack.

Victims of ransomware can find themselves and their business at the mercy of hackers.

Battling Ransomware Part II: How to Respond to a Ransomware Incident

So, you've been hit by a ransomware attack. You're not alone

Ransomware has been around for a few years now, though it wasn't until the quick spreading WannaCry attack in 2017, which affected the British National Health Service, FedEx, and Honda, among others, that it burst on to the scene. Several more high-profile attacks followed, catching many organizations off-guard.

There are several things you can do to mitigate the threat of ransomware and prevent it from gaining hold on your network, but if you've already been infected then it's too late for that.

We'll look at how to prevent ransomware in part two of this article, and it's vital that you do take steps to prevent a reoccurrence, but for now, let's focus on dealing with the problem at hand. Here's a step-by-step look at how to respond to a ransomware incident.

Step 1: Isolate the infection

Many strains of ransomware will try to spread across your network and infect as many machines as possible, so it's vital to act quickly when you detect an attack and try to shut down that lateral movement. The simplest way to do this is to disconnect your computers, laptops, and other devices from the network. It's not enough to pull cables, you should also consider closing off wireless connections via Wi-Fi, Bluetooth, and NFC. If you act swiftly you may be able to contain the attack and minimize damage.

Step 2: Identify the source of the ransomware

If you can find the original point of entry, it should be easier to track the ransomware on your network. Look for alerts from anti-malware tools, intrusion detection, and any active monitoring you have in place. Search for reports of suspicious emails or ransomware resulting from web browsing – it's also prudent to ask people directly, as incidents like this can go unreported. Be vigilant for suspicious traffic and any increase in file renames on local and network file shares.

Step 3: Assess the scale of the infection

You need to know how far the infection has spread and catalogue all the infected systems. Your search should expand across all shared drives and folders, network storage devices, external hard drives, and USB storage, including USB sticks, phones, cameras, and anything else that might harbor suspect files. You also need to check your cloud-based storage services. It's necessary to map the infection before you can effectively deal with it and ensure that it doesn't get the chance to spread further.

Step 4: Classify the ransomware

The potential courses of action open to you depend on the specific strain of ransomware that has afflicted your system. It's crucial to correctly identify it as quickly as possible. You may be able to find a decryption tool online that will allow you to decrypt any data that the ransomware has encrypted. Once you know precisely what you're up against, and you have the big picture of how far the ransomware has spread, you can take the appropriate action.

Step 5: Act to remediate

The time has come to respond to the ransomware incident and act to get your network back online and your business or organization back to normal operations. Unfortunately, your available choices here are going to depend on several factors. Here's what you can do, from best to worst case scenario:

Plan A - Restore from backup

Ideally, you know the importance of backing up data and you have a pristine, recent backup of all your important files ready to go. Before you pull the trigger, however, make sure that all the files you need are present and correct and verify the integrity of your backups. You will want to completely wipe your infected systems before restoring your files from the backups. After restoring the backups, verify that all of your critical apps and data are restored and working correctly.

Plan B - Decrypt your data

Maybe you don't have a backup, or your backup system has been infected too. In that case, you'll want to locate a decryption tool that can be used to bring your data back. To have any chance of this succeeding, you must correctly identify the ransomware first. Unfortunately, for the freshest strains of ransomware, there may not be a tool available. If you can find one, decrypt your files and check their integrity.

Plan C - Accept the loss

As unpalatable as it sounds, you may have to accept the loss of your data and move on. Wipe the system to fully remove the ransomware and start again. If you decide on this course of action it may be a good idea to back up your encrypted files first, as it's possible that someone may develop a decryption tool for your strain of ransomware down the line, enabling you to decrypt that data at some point in the future.

Plan D – Pay the ransom

There are several good reasons not to pay the ransom, chief among them that there's no guarantee you will get your files back even if you do pay up. Paying ransoms also encourages attackers to continue deploying ransomware because it works. It's also worth bearing in mind that your money may end up being used against you in another cyberattack.

Step 6: Make sure it doesn't happen again

In the next part we'll look at how to prevent ransomware, so you can make sure that this doesn't happen again.

If you've been the victim of ransomware its time to resolve the issue and ensure it can't happen again.

Are You Taking Third-Party Risk Seriously Enough?

Because third parties are often responsible for data breaches, your internal security standards must extend beyond your borders to cover vendors and other external partners.

What do the exposure of 106 million records from Capital One, 11.9 million records from Quest Diagnostics, and 7.7 million records from LabCorp have in common apart from the fact they all happened this year? In each case the breach was caused by a third-party. With the Capital One breach a hacker was able to exploit a configuration vulnerability in the servers of one of its cloud partners. The other two breaches were traced to the same third-party – the American Medical Collection Agency's (AMCA) system.

Data breaches are nothing new. More than 5 billion records were exposed in 2018 alone and third parties were often found to be at fault. The potential cost of a data breach is enormous; even after the breach is cleaned up and the vulnerability shut down, there's the risk of fines, penalties and settlements which can amount to millions. The reputational damage can linger for years.

With a proper third-party risk management strategy in place you can drastically reduce the chance of a breach happening in the first place and limit the impact on your business if it does.

It's an expectation not an option

Ignorance is no defense in the event of a data breach. It doesn't matter if a third-party is to blame – if your company is responsible for the data, then you will be held accountable. Regulators in the U.S. and Europe have made it crystal clear that companies are liable for the data they collect and hold, regardless of the network of third parties involved.

Complying with global regulatory requirements is a constantly evolving challenge. It's important to operationalize data management and security. Start to think of compliance as a journey rather than a destination.

While third-party risk management is especially important in healthcare and finance, where sensitive data and multiple partners are par for the course, it also applies to other industries from manufacturing to retail to entertainment and beyond. Outsourcing expands your potential attack surface and heightens your exposure to risk and so it must be scrutinized from the start.

Asking the right questions

While you can dig into technical guides like NIST's CSF and ISO 27001 to help you build solid information security strategies and policies, third-party risk management should start with some simple questions. The best and most obvious way to reduce third-party risk is to limit what you share in the first place. Start with these questions:

- Why are you outsourcing this particular service or data?
- What precisely is being shared and does it all need to be shared?
- Are you doing everything you can to encrypt or anonymize data?
- Does the third-party in question subcontract to others?
- Where are their data centers based?
- What kind of contract do you have in place?
- What are the provisions in the event of a data breach or a service failure?

A robust incident response plan is vital and it should clearly delineate the process for dealing with a suspected data breach, which includes who is responsible for what, a realistic timeline for reporting and remediating, and clear lines of communication. It's alarmingly common for a relatively small incident to snowball into a major disaster because the initial alert was not properly flagged or dealt with in a timely manner.

Regular vendor assessment is crucial

You can't take it on trust – third parties must be thoroughly vetted and regularly assessed. Proper third-party risk management requires clear documentation covering due diligence, detailed risk assessments, a map of third-party relationships, and clear incident response requirements. You should also be generating performance reports and conducting regular audits.

Everything must be laid out in black and white in a watertight service-level agreement (SLA) to ensure you are fully compliant with regulatory requirements. If the worst should happen, then you will be expected to show regulators your workings. Failure to properly interrogate contracts and third-party practices, or to monitor them on an ongoing basis, will be frowned upon.

The problem with traditional vendor assessments is that they tend to rely on a rating system that gives you an easily digestible score or rank, but an arbitrary number doesn't tell you enough about your potential exposure or how to deal with it. It's also fairly common to only conduct reviews annually, but you need real-time rolling visibility if you really want peace of mind.

Acting on the results

One final vital component in successfully managing third-party risk is acting on the information you gather. It's all well and good regularly auditing your vendors or even instituting continuous monitoring, but it's not going to have a positive impact unless your insights are actionable. Each failing must be accompanied by a remediation plan and the remediation efforts themselves must also be assessed to ensure the problem has been adequately dealt with.

In extreme cases, where remediation has been unsuccessful, or vendors repeatedly fail to meet your agreed upon standards, your contract should have provision for you to terminate, without penalty, and find a better partner. If you don't take third-party risk seriously and ensure that your standards cover data internally and externally, then you are undermining your security efforts and there's a good chance you'll end up paying a high price for it.

- Why are you outsourcing this particular service or data?
- What precisely is being shared and does it all need to be shared?
- Are you doing everything you can to encrypt or anonymize data?
- Does the third-party in question subcontract to others?
- Where are their data centers based?
- What kind of contract do you have in place?
- What are the provisions in the event of a data breach or a service failure?

A robust incident response plan is vital and it should clearly delineate the process for dealing with a suspected data breach, which includes who is responsible for what, a realistic timeline for reporting and remediating, and clear lines of communication. It's alarmingly common for a relatively small incident to snowball into a major disaster because the initial alert was not properly flagged or dealt with in a timely manner.

Regular vendor assessment is crucial

You can't take it on trust – third parties must be thoroughly vetted and regularly assessed. Proper third-party risk management requires clear documentation covering due diligence, detailed risk assessments, a map of third-party relationships, and clear incident response requirements. You should also be generating performance reports and conducting regular audits.

Everything must be laid out in black and white in a watertight service-level agreement (SLA) to ensure you are fully compliant with regulatory requirements. If the worst should happen, then you will be expected to show regulators your workings. Failure to properly interrogate contracts and third-party practices, or to monitor them on an ongoing basis, will be frowned upon.

The problem with traditional vendor assessments is that they tend to rely on a rating system that gives you an easily digestible score or rank, but an arbitrary number doesn't tell you enough about your potential exposure or how to deal with it. It's also fairly common to only conduct reviews annually, but you need real-time rolling visibility if you really want peace of mind.

Acting on the results

One final vital component in successfully managing third-party risk is acting on the information you gather. It's all well and good regularly auditing your vendors or even instituting continuous monitoring, but it's not going to have a positive impact unless your insights are actionable. Each failing must be accompanied by a remediation plan and the remediation efforts themselves must also be assessed to ensure the problem has been adequately dealt with.

In extreme cases, where remediation has been unsuccessful, or vendors repeatedly fail to meet your agreed upon standards, your contract should have provision for you to terminate, without penalty, and find a better partner. If you don't take third-party risk seriously and ensure that your standards cover data internally and externally, then you are undermining your security efforts and there's a good chance you'll end up paying a high price for it.

The 7 deadly sins of endpoint detection & response

Breaches often take weeks or even months to uncover, but the right strategy combined with strong endpoint detection & response (EDR) tools can make all the difference. We examine seven vital factors to consider.

There are a lot of different elements that need to come together for an organization to secure its data properly. Most companies adopt a security strategy that focusses on prevention, but the idea that you can completely lock down your systems and prevent successful incursions is a fallacy. Data breaches are every bit as inevitable as death and taxes.

Almost all organizations are going to suffer a breach at some point, but the cost of that data breach depends largely on how quickly it is discovered. The longer it takes to detect, the more expensive it will be, so the fact that it takes companies 196 days on average to detect a breach, according to the Ponemon Institute, is cause for concern.

Swift detection & response is vital, because it gives attackers less time to dig in and move laterally through your network, it reduces the risk of regulatory fines, and it helps you avoid reputational damage. To achieve that speed, you need to get into the right frame of mind and adopt the best EDR tools. To assist you in your task, we're about to outline the seven deadly sins of detection & response.

Lack of endpoint visibility

The average IT environment today includes countless devices running different operating systems. Complexity is growing as the IoT, remote workers, and third-parties add more potentially exploitable endpoints into the mix every day. Every organization needs to take steps to secure unmanaged devices and eliminate the IoT blind spot. Complete real-time visibility into every endpoint on your network should be a priority.

Failure to analyze data

Maybe you've deployed a great EDR system and it's configured correctly, but now your security team is buried under an avalanche of incoming data and they're struggling to pick out the valuable insights that need to be acted upon. There are really two issues here: You need the right tool for your business, properly configured, and you need the resources to analyze the incoming data.

Ignoring alerts

Like the boy who cried wolf, any security tool that churns out a high volume of alerts that include false positives runs the risk of switching people off. When alert fatigue kicks in, security teams start to ignore things that merit further investigation. It's impossible to cull all the bogus alerts, but you have to work to make sure that legitimate alerts don't pass by unnoticed. If it turns out that a genuine issue was ignored, then you need to take a hard look at your procedures.

Overreliance on common indicators of compromise

Whether it's a virus signature or a domain name with a shady reputation, there are certain indicators of compromise (IOCs) that offer a shortcut to uncovering a breach. By all means watch out for these IOCs, but don't rely on them solely. Smart attackers know the IOCs just as well as you do and they're adept at obfuscating and disguising their attacks. Monitoring for suspicious behavior and unusual patterns should also be a part of your defense strategy.

Lack of qualified talent

We know the cybersecurity skills shortage is a major issue for every organization and it's getting worse with every passing year, but even the best EDR tools in the world are going to prove ineffective without qualified analysts behind them. People with the right skills can sift through the data, reduce false positives, and help you squeeze real value from your EDR defenses. Your IT department is probably overstressed, so look to bring in expert services to lessen the load and fill the talent gap. Outsourcing and consultancies can help detect and mitigate problems and run due diligence to deliver the insights you need.

Failure to outline response

It's all well and good being able to rapidly detect a breach, but if it's not swiftly followed up with the necessary action, then it's not helping your organization. A clear triage strategy is required to ensure that serious breaches are dealt with immediately. Set stringent guidelines for reporting and investigation, set clear responsibilities and make sure that the findings inform and drive remediation plans in a timely manner. It's easy to make a bad situation worse if you lack a clear policy that's properly enforced.

Forgetting to measure and improve

The pursuit of security is endless and there's always room to improve your strategy. No matter which tools and expertise you employ, it's crucial to measure their effectiveness. If your team can't handle the alert volume, then give them more resources or find a way to prioritize those alerts more effectively. If there's a big gap between discovery and remediation, you need to set targets and find ways to close it. Work out which metrics are most important to your business and create a feedback loop so that they drive continuous improvements in your strategy.

Most organizations are going to be guilty of a couple of these sins; some may even be guilty of all of them. Repentance is not enough. If you want to improve your detection & response times, then you need to act. Establish visibility, assign the right talent and resources to properly analyze data and alerts, employ sophisticated and varied monitoring techniques, learn from your mistakes and always strive to improve.

7 Tips for a Successful Security Awareness Training Program

When we hear the word "cybersecurity" a lot comes to mind -- firewalls, antivirus, endpoint protection, email security, web security and much more. But how often do we think or talk about people? This is a central element in cybersecurity that is often ignored.

'To err is human' -- it's obvious that as humans we often make mistakes. And we can't be programmed either. As humans our behavior is largely unpredictable and failure to account for insider threats can result into costly security incidents.

Insiders Cost Companies Millions

According to a recent survey by the Ponemon Institute, the average cost of insider-caused incidents is $8.76 million -- more than twice the $3.86 million global average cost of all breaches in the same year. The 2019 Data Breach Investigations Report (DBIR) also highlights that a third of data breaches (34%) involved internal employees.

Cybersecurity is no longer a technical problem. It's a people problem. And ensuring that people have the know-how to defend themselves and the organization against threats is a critical component of a robust cybersecurity program. If the intent of any organization is to comply with regulatory and industry regulations such as FISMA, PCI, HIPAA, or SOX, then it must provide security awareness training in order to meet compliance obligations.

Implementing A Robust Security Awareness Program

The end goal of establishing a thorough program is not to meet compliance requirements. The main goal is to prevent loss of sensitive data and the pain and costs that follows a cybersecurity breach.

As Stu Sjouwerman, CEO of KnowBe4, the world's largest security awareness training company (and Towerwall partner), explains in his book, Cyberheist: The biggest financial threat facing American businesses since the meltdown of 2008, "Security awareness is the essential counterstrike against cybercriminals, and it's the key to avoiding crimes in almost every case. For the best protection, make security awareness training an essential part of your defense-in-depth strategy and require training for all employees."

Here are 7 effective tips to help you put an effective cybersecurity program into place.

1. Evaluate the threat landscape

Evaluation of your critical assets is usually the first step in developing your wider security awareness program. Such an assessment can range from anything like a company-wide cybersecurity questionnaire or a phishing test and use the results to roll out a larger program that can be used to target problem areas that are identified in the assessment.

2. Train employees to recognize a phish

A recent Microsoft Security Intelligence Report claims a massive 250% increase in phishing attacks from the previous year, indicating that phishing attacks are now by far one of the most frequent attack vectors in an organization. Teaching employees to recognize phishing emails and social engineering attacks is fundamental to any security awareness training program. It's also important to stress the impact employee actions may have on the organization. Phishing simulators are available in the market that can help pin-point weak spots in the organization and it's a good idea to deliver training to these vulnerable employees via different methods.

3. Get creative with content

To spark any form of interest in large or small organizations, it is very important that your content is engaging. As humans, we are more inclined to remember stories that evoke images and content that engages our emotions, trigger our imagination and motivate us into action. It might also make sense to fine-tune content based on different types of audiences, considering that standard off-the-shelf training may not be suitable for all.

4. Training is a continuous process

As a security officer, you probably want to set-up an ongoing training program. This would mean setting up a curriculum that covers most security threats and that keeps security top-of-mind via a regular cadence of current topics and trends. Training programs can be established at the time of on-boarding a new employee, and any time is a good time to post and share headline-grabbing mainstream data breach news stories as a way to keep security top of mind.

5. Turn to data to measure effectiveness

Having a process to measure training and awareness effectiveness is essential. One approach to measure the impact of training is by counting the number of security incidents that have befallen your organization before you implement your formal training program and then quarterly afterwards. Another approach to measure awareness can be the comparative volume of security incidents being reported by employees. From a content perspective, one can look at participant rates and class feedback to assess if training content is engaging enough or needs modification.

6. Ensure your program is compliant with regulations

Regulations like HIPAA, PCI DSS, etc., can help establish best practices and processes that are required by several federal and state regulations. Making sure your program is compliant with these regulations can help heighten your organization's security effectiveness.

6. Ensure your program is compliant with regulations

Any cultural change starts at the top. Getting upper management buy-in ensures increased support from multiple groups. Not only is it a good idea to establish a regular cadence of communications to alert users about security awareness but it also might also be interesting to recruit C-level

executives to send out alerts occasionally to emphasize the priority of this cultural change.

To sum up, security awareness training is one of the most effective measures against the growing cybersecurity attack menace. By imbibing these tips in your awareness program, you'll be on your way to helping employees avoid being the weakest link and instead able to recognize potential incoming threats and make the right decisions.

In these times of high-risk cyber threats it pays to have well trained staff that can recognize threats.

Other eBooks from Towerwall

20 Critical Security Controls As Proposed By The Center for Internet Security

This eBook strives to make the 20 security controls as described in detail by the SANS institute more accessible to everyday business people. Taking any one of these 20 actions on the list will have a positive impact on your security status, but the smart move is to work towards fulfilling all 20 of these recommendations.
Let us be your partner on this path to securing your networks.

Learn More >>

How to build a Security Operations Center (on a budget)

Security Operations Center (SOC) teams are responsible for monitoring, detecting, containing, and remediating IT threats across critical applications, devices, and systems in their public and private cloud environments as well as physical locations.

Learn More >>

For even more resources check out https://towerwall.com/tools_insights/whitepapers-ebooks/