The New Breed of Cybercriminal

What You Can Do To Protect Your Business From Being Held Hostage, From Lost Profits And From Reputational Damage

Xact IT Solutions
There are no IT problems.. only IT solutions

Provided as an educational service by
Xact Cybersecurity and I.T.
www.xitx.com | marketing@xitx.com

THE NEW BREED OF CYBERCRIMINAL

What You Can Do To Protect Your Business From Being Held Hostage, From Lost Profits, And From Reputational Damage

In this report, you're going to discover the most dangerous lie you might believe that's putting you and your organization at risk. You'll see that the true cost of a cyber-attack goes far beyond paying ransomware, how AI emboldens cybercriminals, and what you can do to protect your company. Finally, we'll reveal a truly disturbing fact that might keep you awake at night and that you need to be aware of.

First, a little bit about us and why you should keep reading. My name is Bryan, a husband and a proud parent of two. My company, Xact IT Solutions has been serving businesses for about two decades now. I love what I do because I get to help people just like Mike Debowes. Mike came to me because he needed help in navigating a complex email migration from his previous service provider which suffered a ransomware attack.

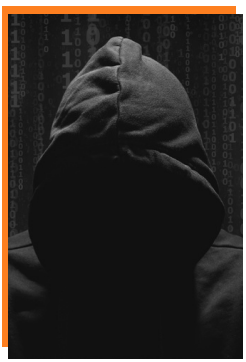
But here's the bottom line. This isn't about my clients or me. **It's about you.**

I am going to start with the most dangerous lie you have been led to believe, and a lot of businesses believe this: "My business is too small for cybercriminals to care about."

That Is A Lie, And Here Are The Facts

Your small business is more likely to be attacked than a large business.

> *One in five small businesses fall victim to cybercrime each year, and that number is growing.*



CEOs and CFOs are now an extremely attractive target for cybercriminals via a tactic called "whale hunting" that specifically targets high-profile employees.

We are also seeing exploits by what are called "drive-by hackers" popping up everywhere. Even though you may have a small business, your business may not even be their main target. What they do is they use you to access businesses higher up on the food chain. They'll infiltrate your business and get information that helps them attack a larger business that you might be working with. They steal from you, they cause damage and then they move on.That's why they're called drive-by hackers.

HOW TO CALCULATE THE TRUE COST OF A CYBER ATTACK?

Next, let's go over the true cost of a cyber-attack. Well, we all know ransomware, and what I call a baby hacker might only ask for $5,000, but other hidden costs exist. The new breed of hacker has a sliding ransomware scale. Here's what that means. **This is important.** The hacker, once they're in your system, finds out what your insurance policy is, what your insurance policy will pay, and possibly how much is in your bank account, and they adjust their demand based on that number. This means they may come in with a preconceived idea of how much they want, but then they say, *"Look at how much this person's insurance company will pay out. Look at how much money they have in the bank. We're going to increase our ask."*

And here is a frightening fact. *Many insurance companies are no longer offering cyber insurance because of the rapidly rising claims. And another fact. Fifty-one percent of all insurance claims are either denied or underfunded because unless your company follows the cyber security protocols in your policy to the letter, to the T, the insurance company will deny your claim.*

Let's say they don't even deny your claim – the insurance company still has the right to send in a forensic team. And when they do that, they're treating your business like it's a crime scene and they shut you down. The first cost is ransomware. But a huge hidden cost that most people don't think about is lost productivity. I want you to do this simple exercise. Divide your annual payroll by 2,080. That's the number of working hours in a year. It's really important because this will be eye-opening for you. That's your hourly cost. If you multiply that by eight, that's how much money you're losing daily in productivity. **And here is the scary fact: this can go on for two weeks, three weeks, four weeks or even more.**

Look at that number again and ask yourself, *"Can my business even survive if I was down for that long?"* And by the way, that doesn't even take into account lost sales. So, go back to that number. What would the real cost be if you were completely shut down for two weeks? No sales coming in. Still having to pay for everything. What would the real cost be over a two-week period?

51% *insurance claims are either denied or underfunded*

2080 *divided your annual payroll, and that is the number or working hours a year*

REAL-LIFE CASE STUDIES

Let me tell you a true story. There was a dentist's office, and the dentist was hacked and all of his patient records were compromised. Obviously, this is a serious violation of HIPAA and it triggered a federal government response. What does that mean? It means the FBI swarmed his practice. They locked his doors. And they went through all his files and computers and more, and he was shut down. **That's what I call a bad day.**

Now, on top of all that, in most states, you must notify everyone in your database that your network has been breached and their data has been sold on the dark web. **This leads to the third cost** of a cyber-attack, and that is damage to your reputation. It is obviously a huge black eye for your company. Imagine getting call after call after call from irate customers, clients, or patients. And by the way, if this breach is big enough, the press will attach itself to it. Imagine waking up in the morning, turning on the morning news, and seeing that your company is the featured story. And **not** in a good way. Of course, your competitors will love this, won't they? And they will jump all over it.

Here is another example of where it happened to a law firm. The law firm found out that they were attacked, and they had to shut everything down. They needed to inform their clients, opposing counsel, and other law firms, and they had to let the courts know. **On top of all that,** they were completely locked out of their clients' files. And aside from the embarrassment, the loss of trust was devastating. You might be able to withstand the ransomware payment and being down for a couple of weeks, but the hit to your reputation lasts for a really long time. And on top of all of that, this law firm was down for two weeks. They couldn't do business for two weeks. So again, review what you wrote down regarding the cost. If you were down for two weeks…what would that mean for you and your business? ***Realistically, could you survive?***

By the way, this particular law firm thought it could never happen to them. They had protocols in place. Well, they ***thought*** it could never happen to them – until it did. You see, the other cost that goes beyond the loss of revenue is the embarrassment of appearing stupid or irresponsible, and that's probably not the case, but that is the perception. And there's the loss of clients for not protecting their data. Class action suits and individual lawsuits. Legal fees to handle the breach compliance lawsuits, plus fines for noncompliance. And then, of course, we've got replacement of data that's corrupted or locked.

AI: CYBERCRIMINALS' FAVORITE (AND EASIEST) WEAPON TO DESTROY SMALL BUSINESSES

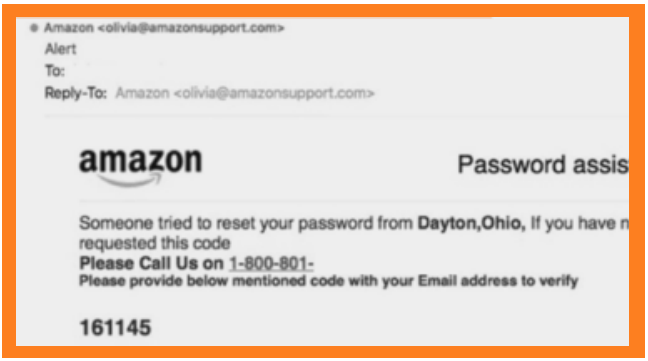
So, now you're fully looped into the cost of an attack and the hidden costs of an attack.

Next, I want to share the impact of AI on cyber security. Obviously, AI is all the rage. It's all over the news. And guess what? **Cybercriminals are loving it.**

We've all heard of deep fakes, where they use a computer program and AI to create an image that looks like something else, or they create an actor saying something that they didn't actually say. You may have even seen this deepfake of the pope and his really, really cool jacket. People actually thought the pope was wearing that jacket. Now, we may chuckle and we may smile at that, but not all deepfakes are funny.

Let me tell you a story of a mother's nightmare. This mother thought her daughter got kidnapped because cybercriminals took just a snippet of her voice from a conversation she had and they used that to fake her voice. They called the mom and played the recording of the fake voice. Now, the daughter was fine, but the mom didn't know that, and they demanded ransom. ***Can you imagine?***

We also have phishing. In the past, you could easily know when an e-mail was fake – for example, because they were poorly written, there were misspellings, and things like that. But I can turn a poorly written phishing e-mail into a nearly undetectable e-mail.



In fact, **look at this e-mail** right now and see if you can spot why this is a fake phishing e-mail. If you or one of your employees clicks on an e-mail that looks like this, your network can be infiltrated. They can get your credentials. And guess what? They're going to use them.

Another common issue with AI is called **encryption breaking.** And this is unbelievable. I saw an expert actually do this onstage. This AI expert took encrypted passwords and did this as a demonstration, using encrypted passwords that are found on the dark web. He fed them into an AI engine and asked the AI engine to break the encryption. And it did – meaning even encrypted passwords can now be broken with AI.

And one of the most frightening new phenomena is infected websites. The new breed of cybercriminals will hack into legitimate websites. Not those fake websites where you see them and you know it's a fake website. No, legitimate websites from big companies. And they'll embed a virus on that website, so if you click anything, or download anything, that virus is now in your network. It's now on your computer.

This new breed of cybercriminal is also doing a lot of texting. Yes, they're still using e-mail, but they know everybody's got their phone. What the hacker will do is send a malicious text to your device and hack in. And then, when you click on the link, it gives them access to all the data on your phone. Now, I don't know about you, but I've got a lot of business stuff on my phone that I would not want the hacker to get access to – bank account information, websites, contacts, health information. All that can be sold on the dark web or used against you. So, now you need to be wary about any text messages from an unknown number.

These are some common ways hackers are using AI, and they use this phishing scheme to get your personal information, to get your money, to get access to your data. And here is what's frightening: an employee will click on one of these links in an e-mail or in a text or download something from a website and do it completely legitimately, thinking they're helping. There's no maliciousness on their part whatsoever, but the damage will still be done.

THOSE THAT HAVE BEEN HACKED AND THOSE THAT WILL BE HACKED

The truth is that the new breed of cybercriminal has more ways than ever to attack you. And speaking of that, here is a scary fact you're probably not aware of but that you need to be aware of.

This is a big one. The new breed of cybercriminal will infiltrate your network and then they'll not do anything for weeks, meaning they'll plant a virus on your computer and they'll just let it sit there. They'll let it do its work. It will scan information, get the information that it needs, and it could be on there for a week or even a month, and you are not even aware of it. And then, when the time is right, when they feel you are most vulnerable, they'll unleash that virus, and it's like a ticking time bomb. A ticking time bomb that could be in your network right now.

Are you 100% certain, without a shadow of a doubt, that your network hasn't already been infiltrated? **Robert Mueller**, the former director of the FBI, said there are only two types of companies – those that have been hacked and those that will be hacked.

Now that you understand how the new breed of cybercriminal is working and what you can do to protect your business and yourself, **I have some good news**.

There are three key things you need to be aware of when it comes to what you can do:

- **protect**
- **detect**
- **respond**

Let's talk about the first piece, which is **"protect."**

What you're looking to do is make your business less attractive to cybercriminals. Think about it as an alarm system for your house. If you have an alarm system and you have the sign up that says, **"This is protected by XYZ Company,"** the criminals know you have a sophisticated alarm system in place that's going to alert the police immediately and that's going to start shining lights and having sirens go off, so they're less likely to rob your home. It's the same thing here. We want to make your business less attractive to cybercriminals.

How do you actually do that? The first step is to ensure that you have the most up-to-date cybersecurity protocols and technology in place.

The hackers are getting more and more sophisticated **every single day,** and the tools they're using are getting more and more sophisticated. It is mission critical that you keep up with them by making sure your technology is the best and the most up-to-date and the most powerful possible.

The second thing is to have **comprehensive training** for your employees and yourself about what to look out for. A lot of C-level executives will say, "Well, I don't need the training because they're not going to come after me." But sophisticated cybercriminals love to go whale hunting for high-profile employees and CEOs, and comprehensive training about what to look out for, what security measures to put in place, and what to do and what not to do are so important to making your business less attractive to the cybercriminal.

Here's a secret that many cybersecurity companies don't want you to know. If a sophisticated cybercriminal wants to infiltrate your network, they'll find a way. That's the bottom line. You could have the best technology in place and have comprehensive training for yourself and your employees, and you need all of that because it will make your business less attractive.

But if the new breed of cybercriminals wants to get into your network, they're going to find a way to get in.

That's why early detection is mission-critical. In fact, out of the big three – protect, detect, and respond – **detection** is the biggest and most crucial element of all. Rapid-fire detection is vital to minimizing potential damage by shutting down hackers as quickly as possible. So, when they infiltrate your network, you immediately know it and you can take the actions you need to take to mitigate the damage and stop it in its tracks.

An aside: if an IT company tells you they can prevent you from being hacked, they're not telling you the truth. That's why at Xact Cybersecurity and IT, we continue to invest in the most up-to-date, powerful DETECTION technology available.

Now you know how to protect yourself by having the most up-to-date technology in place, comprehensive training for yourself and your employees.

Next up is a **quick response** and why that is so important. As I mentioned, fast response begins with early detection. That's why detection is the most important of the big three. You see, once we detect a threat, our sophisticated software can quickly determine and eliminate the root problem.

You need to make sure that you not only have quick detection, but that your IT company and your cyber security company respond quickly to it, because faster response means less damage and, in some cases, can eliminate all those negative consequences we talked about.

WILL THEY CALL YOU STUPID? OR IRRESPONSIBLE?

I want to go back to the most dangerous lie you might have believed that is putting your organization at risk: **"My business is too small for a cybercriminal to care about."**

But here's the bottom line.

If – and actually when, as Robert Mueller would say – your business falls victim to a cyber-attack, depending on what happens, you will be blamed. There's no sympathy for a hacked business, and you're wrongly labeled as irresponsible and stupid. And if and when your business falls victim to a cyber-attack, depending on what happens, you may be questioned, possibly even investigated, about what you did to prevent that from happening.

If and when your business falls victim to a cyber-attack, depending on what happens, you may need to notify all your clients that their data was exposed. You could lose files, you could lose data, delaying projects and halting services. And if and when your business falls victim to a cyber-attack, depending on what happens, if it's in the news or your competitors get wind of it, they will have a heyday destroying your reputation. Finally, if and when your business falls victim to a cyber-attack, depending on what happens, the cost of restoring data and work can quickly escalate.

But I want you to understand this one thing.

WHILE THE NEW BREED OF CYBERCRIMINAL IS BECOMING MORE AND MORE SOPHISTICATED, SO. ARE. WE.

You **CAN** protect yourself from being a victim of cybercrime, and there are three steps to protecting your organization now.

STEP 1

A threat assessment. What's lacking in your security right now? Are your systems really backed up? Where are you exposed to risks? This threat assessment absolutely needs to be done by an independent third party. Just as you can't proofread your own work, your current IT company can't and shouldn't do the threat assessment. A third party needs to do this.

STEP 2

Create an action plan and implement it. Based on what is discovered from the threat assessment, an action plan is created and implemented to protect you if and when an attack happens. And again, this prevents you from being an easy target.

STEP 3

Ongoing maintenance. You don't want to take a set-it-and-forget-it approach to security, because your hackers won't. This isn't a one-and-done thing. You need to have ongoing support, ongoing monitoring of your systems.

FREE And Confidential Cyber Security Risk Assessment Reveals Where Your Company Is At High Risk Of Ransomware, Hackers And Other Devastating Cyber-Attacks

I want to introduce my first gift to you of a **Cyber Security Risk Assessment.** Before I tell you about this, let me tell you who this is not for. This is not for you if you are a one-person company. If you're one person in a business, this is not something you really need. This is not for you if you fear putting your current cyber security company or IT department to the test. This is not for you if you don't feel that protecting your business from the new breed of cybercriminals is a priority. If, after everything we've talked about, you say, *"Oh, I don't really care about this, this can't happen to me"* – then this isn't for you.

Let's talk about the Cyber Security Risk Assessment and how it works. First, there is a 15-minute initial phone call to discuss your company and determine if the assessment is right for you. If it is, we'll let you know in detail how it works. Then, if we decide an assessment is the appropriate next step, we'll do the assessment and then present our findings and show you where your network is at risk if a gap does exist.

With the assessment, you're going to know the following:

- If your login credentials or your employees' credentials are being sold on the dark web. And here's something you may not want to hear, but it's the truth: *I can practically guarantee one or more are.* And what you're going to discover in this report will shock you.

- If your IT systems and data are **truly** secure from hackers, cybercriminals, and rogue employees – and again, most employees want to do a good job, but there are those rogue employees who are out to hurt you – you'll know that as well. We'll also give you a health score for your network to determine if there are any outdated, unsupported, slow, or problematic areas, and we'll tell you how your network ranks against that of other companies of your size in your industry.

- Whether or not your current backup will allow you to restore 100% of your data. We have found that many businesses have a backup, but it doesn't allow them to restore all their data. We'll tell you how fast it can be back up and running if ransomware **locked** all your files. And again, in 99% of the computer networks we've reviewed, they were absolutely shocked to discover that they would not be able to quickly access their data.

WHY FREE?

Now, the good news is the first step is FREE. The threat assessment and dark web scan for your organization has a value of $10, 000 but it is absolutely free.

To get your free threat assessment and to schedule your 15-minute initial call, go to https://www.xitx.com/call/

After the assessment, you're going to make one of three decisions:

- Do nothing and hope that everything will be okay.
- Take our findings and source another cyber security company to help you.
- You'll discuss working with us, which is obviously what we hope for.

To schedule your 15-minute initial call, go to xitx.com/call

You'll be taken to my simple calendar page, where you can select a time that works best for you.

In addition to the no-cost, no-obligation risk assessment, I also have some very valuable gifts for you. Included free is the dark web scan and a report for your personal credentials and your employee passwords. This has a value of $10,000 and you are going to be shocked by what we dig up. And it's obviously 100% confidential.

The next thing you receive is one of my best-selling books, Checkmate. In this book, you'll learn how just one cyber attack can cause you to lose control of your business and what you can do about it.

You're also going to get a copy of my book "Under Attack" where you will learn how to protect your business and your bank account from fast-growing, ultra-motivated, and highly dangerous cybercrime rings.

Finally, you'll receive, "The Cybersecurity Crisis", a FREE report that explains the critical cyber security protections every business must have in place to protect their client data and reputation.

To get all of this with no risk, and no obligation, simply go to xitx.com/call. Once again, you'll be taken to a very simple calendar page where you can select a time that works best for you for the 15-minute initial call.

Please…Do NOT Just Shrug This Off
(What To Do Now)

Please don't put this off thinking it can't happen to you. The fact is, everyone who has been breached at one point has thought, *"This can't happen to me,"* **until it does.**

The first call is just 15 minutes long. That's to make sure we can actually help you. Then we're going to be talking for about 10 minutes to get the information we need to actually run the assessment, and then you're going to need to dedicate about one hour to go over the results with us. The significant time investment is on **OUR** part rather than on your part.

To schedule your 15-minute call to get this started, go to https://www.xitx.com/call/

I want to just cover some questions I always get asked that you might have.

The first question I get asked is *"Will my current IT company know you're running a risk assessment?"* Here are some things to know. First, you don't want to tell them because the fact is, they should catch that the assessment is being done and alert you. It's a big, big, big, big **red flag** if they don't.

The next thing is, if they're doing their job that you pay them to do, they actually shouldn't worry about it. I wouldn't care if somebody did it for the organizations we protect, because we would know instantly and we would respond instantly. And remember, if everything looks good, if everything is the way it should be if your current IT company catches that we're running this – and they should – fantastic. You know that you've got great cybersecurity
firm and you can sleep well at night.

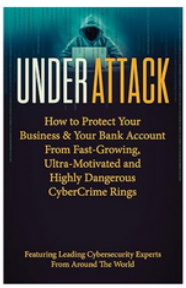
But the third and **most important** reason is that you owe it to yourself your employees and your customers, clients, or patients, to ensure that you are protected. The fact is that our cyber security assessment will help you sleep well at night.

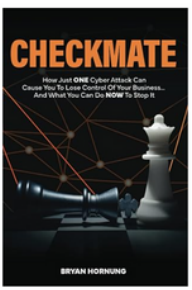
An obvious question that I get is **"Okay, that sounds great. I understand that the assessment is free, but what's it going to cost me *after* the assessment?"** The truth is, it might not cost you anything. If we don't find any problems, there are no problems. We give you the thumbs-up.

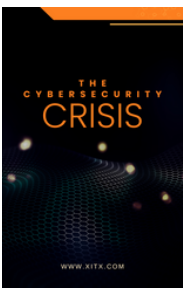
The other fact, though, is that the investment – and it is an investment – to secure your network depends on the complexity of the problems we find in the assessment. Once we do the assessment, I can tell you precisely what the investment is going to be. But the fact is that cyber security doesn't have to break the bank – but the new breed of cybercriminal certainly can.

Another question I always get is **"Why are you doing the assessment for free?"** First of all, there is *no catch*. There is no obligation. You don't have to work with us after the assessment. Obviously, I'd love to earn your business, but there's no pressure to work with us. My mission, and the reason I'm doing this assessment for free, is to ensure that businesses don't become victims of cybercrime.

To summarize, here's everything you get when you schedule your Cybersecurity Risk Assessment: ***Dark Web Scan plus . . .***







So, the total value of this is $10, 000+, but it's all FREE for you when you schedule today.

What Other Business Owners Are Saying

"Absolutely the best IT services in South Jersey. One thing I never have to worry about? My tech. Recommend without reservation." - JEFF KERSTETTER

"The team at Xact IT Solutions responds quickly and completes requests efficiently. We are very happy with Xact It as our technology partner." - KRISTI HOWELL

"Xact Cybersecurity & I.T. helped us navigate a complex e-mail migration after our previous service provider, Rackspace, suffered a ransomware attack. They were professional, efficient, and ensured a seamless transition with minimal disruption to our business operations. We felt well-informed and confident throughout the entire process. Their service was exceptional, and I would recommend Xact Cybersecurity & I.T. to anyone seeking robust and reliable e-mail and security solutions." - MIKE DEBOWES

If you have any questions about what you read today, we'd like to answer them. On this call we can discuss your unique situation, any concerns you have and, of course, answer any questions you have about us.

If you feel comfortable moving ahead, we'll schedule a convenient time to conduct our Cyber Security Risk Assessment.

Visit:
https://www.xitx.com/call/

Or call us at: 856-651-6509