TARGETS OF OPPORTUNITY:

WHY CYBER CRIMINALS PREFER SMBs AND WHAT SMBs CAN DO ABOUT IT

Enterprise Visions – Twin Cities Office
1030 West County Road E Suite 150
St Paul, MN 55126
651.450.7900

ENTERPRISE VISIONS
DIGITAL TRANSFORMATION SIMPLIFIED

ENTERPRISE VISIONS
DIGITAL TRANSFORMATION SIMPLIFIED

In the era of modern business, cyber crime and data breaches are taken as a matter of course – the cost of doing business. What is very often overlooked, though, is just how high that cost can be. Cyber attacks cost the global economy an estimated $400 billion annually, and that amount is increasing year over year. Given current trends, the projected annual cost of cyber crime to the global economy in 2019 will be in the neighborhood of $2.1 trillion.

Data breaches cost an average of $6.5 million per breach in direct costs for U.S. companies, or an average of $154 per data record stolen. Those numbers are direct costs only, and don't factor in the effects of the loss of trust that so often follows, or the possible liability-related damages that can result from a security breach. Many small and medium-sized businesses (SMBs) are just one phishing attack or unsecured network endpoint away from closing their doors permanently.

That may sound like a hyperbole, but according to Experian, 80% of small businesses that experience a data breach are out of business within 18 months.

In addition to the significant financial costs involved in detection and forensic analysis of the breach, restructuring of the network and security infrastructure, and reporting and reparations to the affected parties, there is also the loss of trust engendered by a data breach. The effects of this loss of trust are undeniable, though difficult to quantify with any precision.

Most small and medium businesses lack the resources to recover from such a scenario.

Enterprise Visions – Twin Cities Office
1030 West County Road E Suite 150
St Paul, MN 55126
651.450.7900

That leaves prevention as the best cure. But modern cyber attacks are so advanced and sophisticated that none but the largest enterprises can afford to levy the talent, manpower, and other resources necessary to keep up and stay safe. For everyone else, keeping up with new security vulnerabilities is a Sisyphean task, almost certainly doomed to fail. New vulnerabilities are being discovered and exploited daily, and all it takes is one chink in the armor for the whole castle to fall.

What is an SMB to do?

In the U.S., SMBs account for the majority of new jobs created, and more than half of all sales and payrolls. SMBs have an outsized impact on the national economy, and that makes them a juicy target.

All is not lost, however. By understanding what motivates cyber criminals to attack SMBs, it is possible to take steps that will help shore up the defenses against them. This white paper looks at why cyber criminals prefer to attack SMBs, and what SMBs can do to mitigate those risks.

UNDERSTANDING TARGETED ATTACKS

The types of attacks that get headlines in the news are those against large enterprises and major players – the kinds of attacks that affect millions of people. This unbalanced coverage can lead to a false sense of the reality, though. Statistics show that the majority of cyber attacks target SMBs rather than big corporations.

And "target" is a key word. Unlike the scattered, drag-net style cyber attacks of yesteryear, modern attacks are customized, focused, and precise. Rather than tossing

Enterprise Visions – Twin Cities Office
1030 West County Road E Suite 150
St Paul, MN 55126
651.450.7900

ENTERPRISE VISIONS
DIGITAL TRANSFORMATION SIMPLIFIED

out an exploit or malware-laden spam email and seeing what it catches, today's attackers target specific organizations, and often are looking for specific information.

What modern cyber criminals do is less cyber attack and more cyber espionage.

They often begin with reconnaissance – scouting out a network, identifying likely locations for valuable data, and mapping out every weak point. From there, it's a grab-bag of possibilities. Email, file systems, mobile connections – bring your own device initiatives have been a jackpot for bad actors – and of course websites are all fair game and full of potential.

Once they are inside the system, the game is over. It's their network now. But they aren't always finished at this point. To make matters worse, a compromised SMB system is often used to gain access to the networks and data of larger partners and bigger companies with whom they do business.

What makes SMBs such inviting targets? The following five factors:

- Data value
- Low risk
- Ease of penetration
- Victims unaware of the danger
- Insufficient security

Let's look at those points in more detail.

Enterprise Visions – Twin Cities Office
1030 West County Road E Suite 150
St Paul, MN 55126
651.450.7900

ENTERPRISE VISIONS
DIGITAL TRANSFORMATION SIMPLIFIED

WHAT IS THAT DATA REALLY WORTH?

Every business has information that is valuable to someone. Credit card records, employee payroll info, and other personal data can be used to generate fraudulent profits. Even the business's banking info is fair game. And most cyber criminals aren't looking for a million dollar heist. It's much safer and easier to chase after a thousand $1,000 scores, and the end result is the same.

Sometimes it isn't even the SMB's data the attackers are after. Sometimes it's their access to another company's data.

Most SMBs do business with bigger companies, and those companies work with bigger companies yet. Sometimes an SMB is just the first step on a longer path to a much larger target.

RISK VS. REWARD

The internet has opened up new markets around the world, and in doing so it has created entirely new ways of doing business – both legitimate and otherwise. While the internet age has enabled companies to connect and do business all over the world, it has also opened them up to attacks. When attackers are physically located halfway around the world, even when they are caught they are seldom brought to justice.

And there's no guarantee they'll be caught. Most of the advanced malware used by professional bad guys is difficult or impossible for standard antivirus software to detect. It can sit around on a system for weeks or months before antivirus updates catch up with the latest exploits.

Enterprise Visions – Twin Cities Office
1030 West County Road E Suite 150
St Paul, MN 55126
651.450.7900

If it isn't detected, most malware will also clean up after itself, leaving no trace that it was ever there as it sneaks away with its valuable data payload.

And that's to say nothing of state sponsored industrial espionage and hacking. Numbers are hard to come by, but there is little doubt that many states bankroll a certain number of cyber criminals who are encouraged to target businesses in other countries.

SMBS ARE EASY TARGETS

SMBs have to deal with the same types and numbers of attacks as larger corporations, but with a very small fraction of the security budget and a fraction of the manpower. Enterprises may have a person for every security role, but it's the rare SMB that can spare more than one person to do everything.

On top of being understaffed and overwhelmed, SMB security departments are also usually unable to implement or maintain the type of layered, in-depth defense that larger corporations use as a matter of course. It probably wouldn't matter if they could. The types of defensive measures that are cost effective for smaller networks and systems are simply not effective against modern cyber-threats.

It is also true that all the security related software and hardware in the world is useless in the absence of solid security policies and procedures, and this is another place where SMBs often lag behind their larger competitors. It may not seem to make sense to have a set of formal security policies or procedures for a small business of only a few people, but that is one of the most often overlooked factors that makes SMBs such an easy target for cyber criminals.

Enterprise Visions – Twin Cities Office
1030 West County Road E Suite 150
St Paul, MN 55126
651.450.7900

ENTERPRISE VISIONS
DIGITAL TRANSFORMATION SIMPLIFIED

SMBS DON'T THINK THEY'RE AT RISK

In spite of the statistics which show that SMBs are likely to be the target of cyber attacks, most SMBs don't consider themselves to be a likely target, and almost half don't prioritize their security.

Many SMBs either don't understand the frequency or sophistication of modern cyber crime and don't think they have anything of value to cyber criminals, or believe that their consumer-grade security measures are sufficient to keep them safe. This is a false sense of security, in particular with regards to the quality of the security tools many SMBs use.

INSUFFICIENT SECURITY TOOLS

The standard arsenal of SMB security tools is simply not up to the task of protecting against aggressive modern attacks. Gateways, firewalls, and AV software are certainly necessary components of any security strategy, but they are insufficient when pitted against targeted attacks.

Most traditional security measures rely on malware signatures and blacklists to function, but these days attacks often make use of dynamic URLs and zero-day exploits. Dynamic URLs make blacklists all but useless, and there is little chance that a commercial AV will have the signatures of most zero-day exploits. Zero-day exploits are, by definition, exploits that are not commonly known to the security industry.

WHAT CAN BE DONE?

Cyber criminals aren't random or stupid. On the contrary, they are generally very well organized, meticulous, and

Enterprise Visions – Twin Cities Office
1030 West County Road E Suite 150
St Paul, MN 55126
651.450.7900

ENTERPRISE VISIONS
DIGITAL TRANSFORMATION SIMPLIFIED

logical. They target SMBs for all of the reasons discussed above and have every expectation of success. What, then, can an SMB do to prevent a successful targeted attack?

BE AWARE OF BEING A TARGET

All SMBs are likely targets, and the greatest advantage the cyber crooks have is that so many SMBs are blissfully unaware of the danger they are in. All businesses have valuable data, and for SMBs that do business with larger companies that is doubly true.

By being aware of the danger and staying vigilant, an SMB can take away that advantage, thereby preventing a successful intrusion or mitigating the damage should someone get through the defenses.

IDENTIFY WHAT'S VALUABLE

Not all data is created equal. With limited budgets and limited capability to resist sophisticated, modern hackers, sometimes it's necessary to focus available resources on some, rather than all, data.

It is not as simple as it sounds to determine what data would be valuable to an intruder, however. Seemingly innocuous information might hold the key to further access, or to unlocking access to other information, in the hands of a clever hacker. Looking at the system from the mindset of an intruder can help to see what data is valuable to cyber criminals and what is not, and can bring to light any weak points in the security system.

Enterprise Visions – Twin Cities Office
1030 West County Road E Suite 150
St Paul, MN 55126
651.450.7900

ENTERPRISE VISIONS
DIGITAL TRANSFORMATION SIMPLIFIED

USE A MODERN SECURITY PLATFORM

Cyber attacks have advanced, evolved, and changed over the years – sometimes at an alarming rate. Security systems have, for the most part, stayed much the same. Attacks don't work the same way anymore, but security does. That gives an enormous advantage to the attackers in this scenario.

By attacking unknown vulnerabilities in novel ways, modern cyber crooks make bypassing signature-based security laughably easy. It's simply not possible to keep these systems updated in a way that makes them useful against new, never-before-seen attacks. They only work against known attacks, known viruses, known malware sites.

What is necessary to keep SMBs safe in the modern era of cyber espionage is a security platform capable of identifying and preventing new types of malicious activity, intrusion attempts, and attacks in real-time. What is necessary is a completely new approach to SMB network security.

Enterprise Visions – Twin Cities Office
1030 West County Road E Suite 150
St Paul, MN 55126
651.450.7900