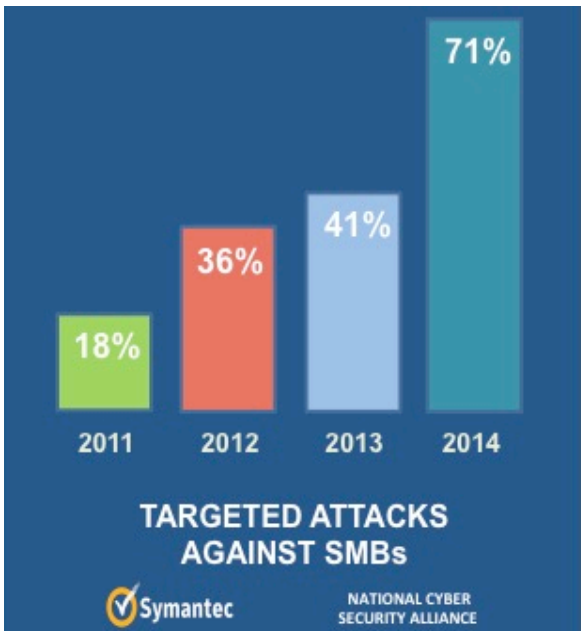
The DynaSis Educational Series for C-Level Executives

Cyber-Security 2016

There seems to be a new cyber threat or attack in the news almost every day. It has reached the point where we don't really even pay attention anymore. And why should we? As business people, we know it's the big guys, the Targets, the Sonys, the Dominos Pizzas, and of course, federal and local governments that are being hit. If you are a Small to Mid-sized Business (SMB) doing less than $10 or $20 million a year in revenue, the cyber-attackers are going to leave you alone, right? After all, they have a lot more $100 million to multi-billion dollar companies to go after. Right?



Bigger fish to fry. Right?

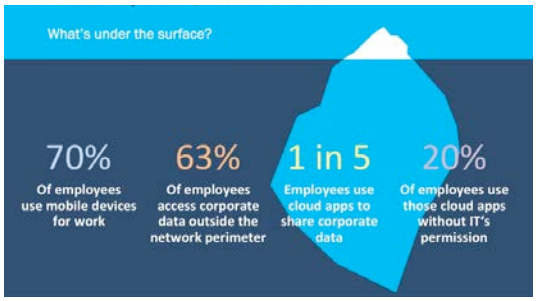
Wrong.

In 2014, the last full year for which we have the statistics, 71% of cyber attacks were against SMBs. What's even worse, over the past few years, 60% of SMBs that suffered a cyber-attack were so devastated by the results of the attack, that they closed their doors within six months. And the rate at which SMBs are being attacked is increasing exponentially.

To give you the best information we know how to provide, this White Paper is broken into two parts. In **Part One** we delve into the changes we have seen in cyber crime over the past few years and why it's happening. In **Part Two**, we discuss preventive measures you can take to protect your business, your employees and your family.

PART ONE: The highly sophisticated cyber-criminal of 2016.

Protecting yourself against cyber-crime used to be fairly easy. Got a problem? Buy a box. In that box was a firewall. We probably didn't know exactly what it did, but we felt safe.



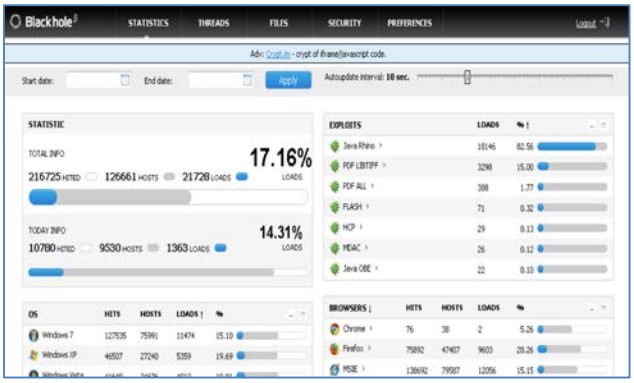
But the way we work today has changed. The people in your company who use your network have left the building! They work from home, on the road, even on vacation. And all this travel has exposed your data, and your business, to new risks. So has the fact that many people now use their own devices – laptops, tablets and smartphones – to do company business and access company files. A more efficient workforce? Sure. But this new efficiency has also led to risk.

To fully understand this risk, you have to understand the evolution of cyber-crime and today's criminal. The diagram on the right shows how in the "old" days of cyber-crime, the cyber-criminal needed his own servers, had to build his intrusion software from scratch, had to invest a lot of his own money, and then identified large targets.

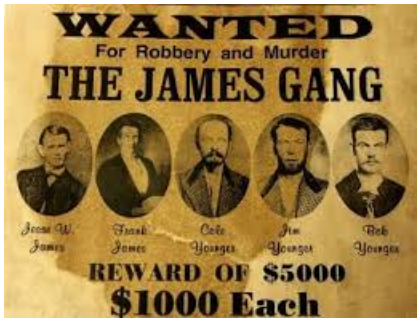
Evolution of Cyber Crime

OLD	NEW
Hacker Organization ▪ Centralized ▪ Build from scratch ▪ Own servers ▪ Expensive ▪ Large targets	**Crime Ecosystem** ▪ Distributed ▪ Buy or hosted ▪ Specialize in areas ▪ Cheap ▪ Smaller targets

Today, the cyber-criminal can actually buy inexpensive "off-the-shelf" Exploit Kits, similar to the way you go online to a large retailer's website and buy the latest version of Turbo-Tax or Photoshop. Instead of working for a large organization that had to spend many months and many dollars creating its hacking software, a small-time criminal has evolved into a stand alone, do-it-yourself techie who visits an online store that actually sells him what he needs to steal your data and destroy your business. And it is easily downloadable and very affordable.



It seems like the criminals of old had a much harder time robbing banks and government agencies. And they often got shot and killed in the process! Today's criminal can rob you from the comfort of his living room, or while sitting on the beach in Barbados.



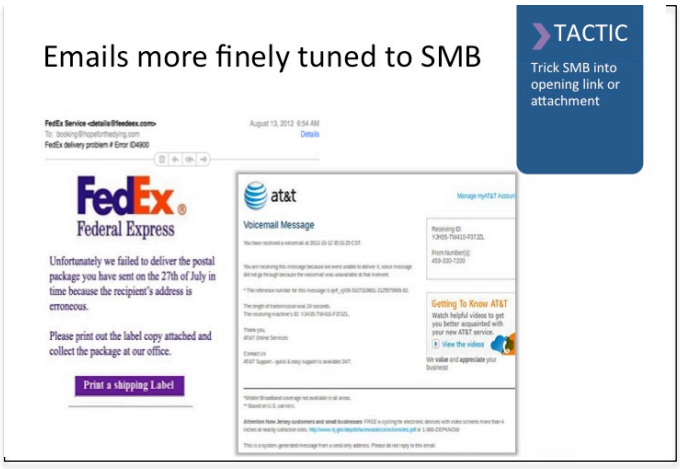
Decisions, decisions! Say I am a cyber-criminal and I just bought my very own package of intrusion software. Now I have to make a big decision: who do I target? There are a lot of big companies out there whose data I would love to grab, but the reality is that most large companies today have spent millions of dollars protecting themselves against small time hackers like me. My off-the-shelf software is not going to breach their protection. But I have a better answer: go after a lot of small companies who have not bothered to set up the layers of protection that will keep me out!

As a budding cyber-criminal, once I have made that decision, what do I do next? I might choose to insert "malware" into your network. Malware is this really clever piece of code that, once it has infiltrated into your system, calls out to the sender and gives him the ability to download your data, and/or encrypt your data so you cannot access it without first paying him a ransom of hundreds, or thousands, or even tens of thousands of dollars. That's not a bad ROI on an investment of $50 to $150 worth of software (training included!)

As scary as the above scenario may be, it's not the only way your business (or personal accounts) can fall prey. As obvious as many phishing ploys seem to be, many people fall for these schemes that infect their devices and open them up to all types of malevolent behavior.

Have you ever gotten a personal email from an African Prince?

Or an "important" message from Fedex or AT&T?



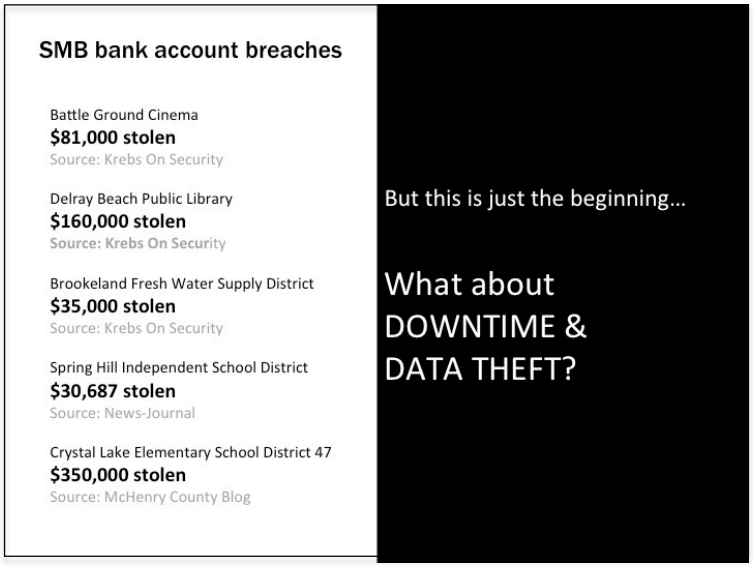
This writer once got an email from a dear friend who was stranded in London and desperately needed $1,500 bail money wired to a European-based bank account before being thrown out of merry old England. Of course, this friend was sitting next to me here in the USA, enjoying lunch at the time, or maybe I would have been fooled, too.

Ryan Kalember, Senior VP at ProofPoint, was recently quoted in TechNewsWorld, "It's probably never going to happen, but it would be fantastic to get smarter users who are less susceptible to social engineering. Nine out of 10 data breaches start with a phishing email", Kalember noted. In order for phishing to work, a user needs to click a link, open an attachment or follow directions that lead to trouble.

"Smarter users would be wonderful if that were a thing that were actually achievable," he said.

If you are saying to yourself that you would never be fooled by the type of scheme, consider this: if any one of your employees does fall victim to any of the above kinds of cyber-crime (and there are more that we have not mentioned), they could be opening your entire company to a breach that will lead to:

- All your customer's personal data being revealed. (Remember Ashley Madison?)
- Your bank accounts being drained.
- New credit accounts being set-up in your company's name and being maxed out before you become aware.
- Your files being "locked" and held for ransom.
- Your business and personal credit being destroyed.
- You and your company being sued.



And here is something else of which to take note:

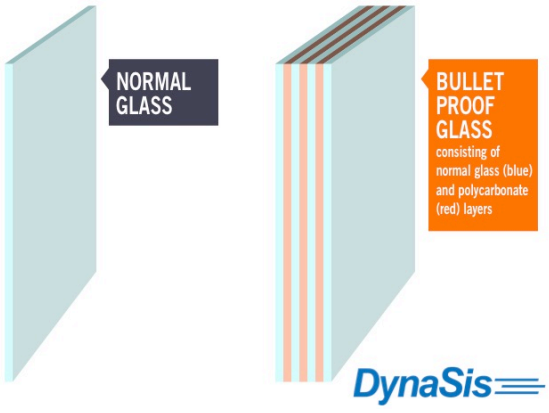
The courts and insurance companies are now taking a dim view of businesses that do not do everything reasonably in their power to protect themselves and particularly their customers from such activity. Business owners who believe their insurance companies will pay out against such losses, or that the courts will find in their favor when they are sued by former clients, are getting some nasty surprises.

PART TWO: PROTECTION AND CONTAINMENT

This is the old "good news – bad news" type of situation. The bad news is that there is no one single piece of software, or device, or change of work methodology that will guarantee absolute protection. Rather, the "good news" is that effective protection can be achieved through a layered approach…kind of like bulletproof glass.

Is it guaranteed protection? No. In today's world, with cyber-criminals working very hard at developing new and more sophisticated ways to attack, you and the your IT service provider have to always be on the alert. You must also have in place the tools for "containment". In other words, your network must be set-up to recognize when a software infection, or intrusion by malware, has occurred, and quickly "contain" it within the areas that have been infected and stop its spread.

Security & Risk Mitigation: a Layered Approach



As we said above, this is best accomplished through a layered approach, so we will briefly outline the steps we feel best accomplish this. The techniques described below were developed by a group of CEOs and Presidents of 12

independent IT service providers from across the country who meet several times a year to share and develop strategies that benefit their collective SMB clients. Because of the unique nature of their collaboration, they are usually ahead of the curve in terms of the advances they bring to the marketplace and their clients.

(Note: This White Paper is intended to be an informative piece designed to help SMBs protect themselves in today's treacherous cyber-environment. It is not intended to be a sales piece for DynaSis. That said, we are proud of the steps we have taken to protect our clients, including being a member of the CEO/Presidents' group mentioned above, but we suggest all small business owners speak with their service providers. We are also happy to provide guidance to any SMB owner who needs assistance.)

Some of these "layers" merit entire White Papers on their own, and much additional information will be available in our weekly blog posts, so please look at this analysis as an overview:

Layer 1: Start with the USER!

The more people you have on your network, the more chances you have for error. User education is vitally important. Things like: be wary of attachments, fraudulent "bank" emails, and password requests. Cyrus Walker, CEO of Chicago-based Data Defenders says research shows approximately 80% of security-related incidents occur as a result of employee behavior.

Layer 2: Email Security

User education is important, but it is also important to stop threats at the "gateway." Block known variants, malware, ZIP files. Employ message analysis, virus protection, and rate control, among other tools.

Layer 3: Weekly Patch Updates

Workstations and servers must be scanned weekly and patches applied on set schedules with immediate patching for major concerns.

Layer 4: Anti-Malware

Must be regularly updated. Real-time scans for known malware. Daily in-depth scans of entire system. Ability to delete/quarantine malware.

Layer 5: Anti-Virus

Anti-virus works by scanning to check for known viruses, then deleting or quarantining them. As virus sophistication grows, identification is becoming more difficult. The daily in-depth scanning of the entire system is important.

Layers 6 & 7: Firewalls & Subscriptions

Firewalls provide perimeter defenses:

- Firewall subscription services include signature-based detection of viruses and can provide Intrusion Detection and other services.

- Configured to allow only known inbound traffic (e-mail, www, ftp)
- Configured for specific traffic to specific endpoints
- Lock down DNS request from LAN to OpenDNS. This prevents malware from using self-contained DNS resolution and enforces OpenDNS policies
- Virus Identification
- Geo Filtering

Layer 8: Predictive Security – OPEN DNS

Stops malware before it gets into your system. Blocks outbound communication from malware to sender. This protection also covers your employees' devices, like laptops and home computers (when using company network.)

Layer 9: Removing Local Workstation Admin Rights

You may get some pushback from your employees, but hold your ground. Doing this reduces the ability for malware to install itself AND prevents employees from installing unauthorized software, especially common on remote devices.

Layer 10: Crypto Prevent

Prevents malware from installing itself in most common locations. (Note: Crypto is the malware that "encrypts" your files, only to be released upon paying a ransom. Also known as "ransomware.")

Layer 11: Crypto Containment

If a crypto virus does manage to get through, and they are tricky little devils, containment software is designed to disable that portion of your files that have been affected, preventing further infection. This reduces the recovery time necessary to get you back up and running.

Layer 12: Secure Data Backups

Critical for recovery after malware attacks. And the most important word here: **"Secure!"**

IT Assessment

Your IT service provider should be able to provide you with a comprehensive IT Assessment that will highlight your security weaknesses and suggested remedies. Assessments like these are critical in todays' technology environment. Remember this: ***You Don't Know What You Don't Know!***

If your IT is run in-house, your IT team should be very grateful for such an assessment and the upgrades it may point to, because it will enable them to better sleep at night (you, too!) and be more productive at their jobs. It is not the goal of a good managed IT provider to replace your in-house professionals, but instead to enable them to be more productive while better controlling costs and increasing your IT ROI.

But more on that in our next White Paper. Check our weekly blog posts at: www.DynaSis.com/Latest