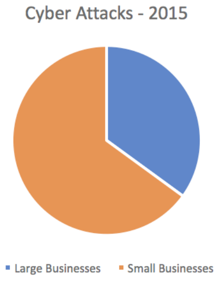
The DynaSis Educational Series for C-Level Executives

Cyber-Security 2017

The DynaSis annual report on the state of cyber-crime and cyber-security.

The big news in cyber security for 2017 was the incredible growth in ransomware attacks last year and how this trend is expected to continue. To understand the magnitude of this problem, let's start with basic numbers. The annual report put out by the SonicWall security team shows this exponential growth:

Attacks in 2014:	**3,200,000**
Attacks in 2015:	**3,800,000**
Attacks in 2016:	**638,000,000**



These are real numbers, not typos. So, yes, that's a **20,000%** increase in a single year. Staggering! While only a small percentage of "attacks" actually get through, ransom payments for successful attacks this year are expected to be in the billions of dollars and, as in past years, the primary targets are expected to be small to mid-sized businesses. In 2015, the most recent year for which we have the stats, 65% of all cyber attacks were against small to mid-sized businesses (SMBs). 65% x 638,000,000 = **414,700,000 expected ransomware attacks against SMBs**. If 1% succeed, that's 6.8 million successful attacks.

We are also seeing a rise in the amount of ransom payments demanded. While consumers may get hit for a few hundred dollars, SMBs are routinely being forced to pay ransoms in the tens of thousands of dollars. Some major corporations and governments have been hit with multi-million dollar ransom payments. You may not be seeing much about this in the media because, very simply, companies do not want the public to know as this can weaken consumer confidence in them.

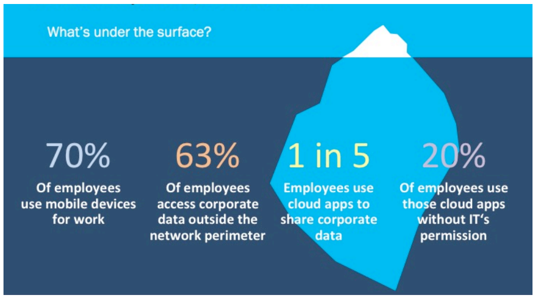
Why SMBs? Larger companies realized some time ago that they needed protection against cyber-crime and have spent millions of dollars fighting this threat. Many enterprise level companies not only have I.T. departments, but have also hired CISOs (Chief Information Security Officers) to work hand-in-hand with their CIOs. In fact, right now one of the most lucrative fields in technology is cyber security, with a current unemployment rate of 0% and almost 1,000,000 jobs going unfilled, and that is expected to rise to 1,500,000 unfilled jobs over the next few years. In the SMB space, the budgets simply are not there for this type of increased in-house protection, and in a state of denial over their vulnerability, many SMBs executive choose to go it alone and hope for the best.

This lack of cyber protection is a vital factor in the growth of ransomware crimes, but it is not the only one. The other big factor is the ease of committing these crimes. Today, the typical kid down the street can dive deep into the dark web and for a few hundred dollars obtain all the software he needs to encrypt the files of a local business (or one around the world) and demand a ransom. There will be more about this later in this paper.

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 2017.

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.



What's under the surface?

70%
Of employees use mobile devices for work

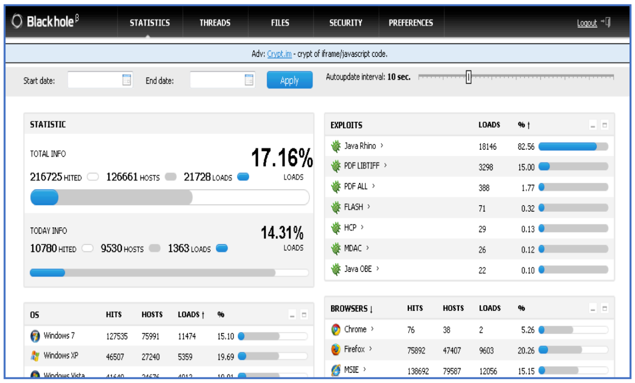
63%
Of employees access corporate data outside the network perimeter

1 in 5
Employees use cloud apps to share corporate data

20%
Of employees use those cloud apps without IT's permission

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 must 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.



Adv: Crypt.im - crypt of iframe/javascript code.

Start date: End date:

Autoupdate interval: **10 sec.**

STATISTIC

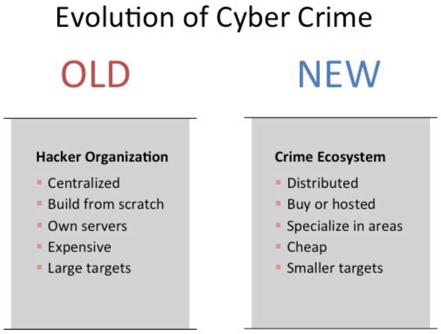
TOTAL INFO
216725 HITED 126661 HOSTS 21728 LOADS
17.16%
LOADS

TODAY INFO
10780 HITED 9530 HOSTS 1363 LOADS
14.31%
LOADS

EXPLOITS	LOADS	% ↑
Java Rhino ›	18146	82.56
PDF LIBTIFF ›	3298	15.00
PDF ALL ›	388	1.77
FLASH ›	71	0.32
HCP ›	29	0.13
MDAC ›	26	0.12
Java OBE ›	22	0.10

OS	HITS	HOSTS	LOADS ↑	%
Windows 7	127535	75991	11474	15.10
Windows XP	46507	27240	5359	19.69
Windows Vista	[illegible]	[illegible]	[illegible]	[illegible]

BROWSERS ↓	HITS	HOSTS	LOADS	%
Chrome ›	76	38	2	5.26
Firefox ›	75892	47407	9603	20.26
MSIE ›	138692	79587	12056	15.15



Evolution of Cyber Crime

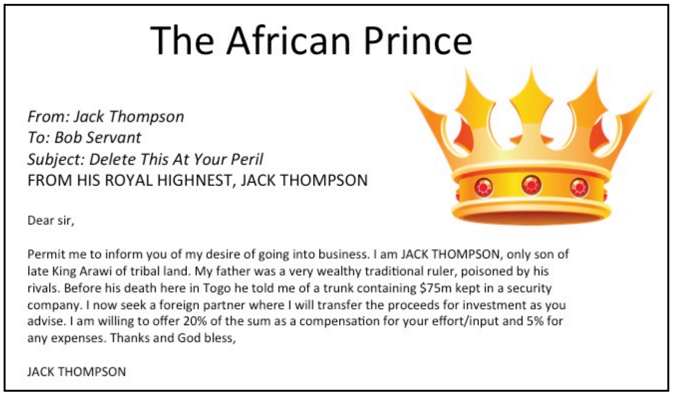
OLD	NEW
Hacker Organization	Crime Ecosystem
Centralized	Distributed
Build from scratch	Buy or hosted
Own servers	Specialize in areas
Expensive	Cheap
Large targets	Smaller targets

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, and includes the ransomware software that has become so prevalent today.

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 since these 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…even technical support!)



The African Prince

From: Jack Thompson
To: Bob Servant
Subject: Delete This At Your Peril
FROM HIS ROYAL HIGHNEST, JACK THOMPSON

Dear sir,

Permit me to inform you of my desire of going into business. I am JACK THOMPSON, only son of late King Arawi of tribal land. My father was a very wealthy traditional ruler, poisoned by his rivals. Before his death here in Togo he told me of a trunk containing $75m kept in a security company. I now seek a foreign partner where I will transfer the proceeds for investment as you advise. I am willing to offer 20% of the sum as a compensation for your effort/input and 5% for any expenses. Thanks and God bless,

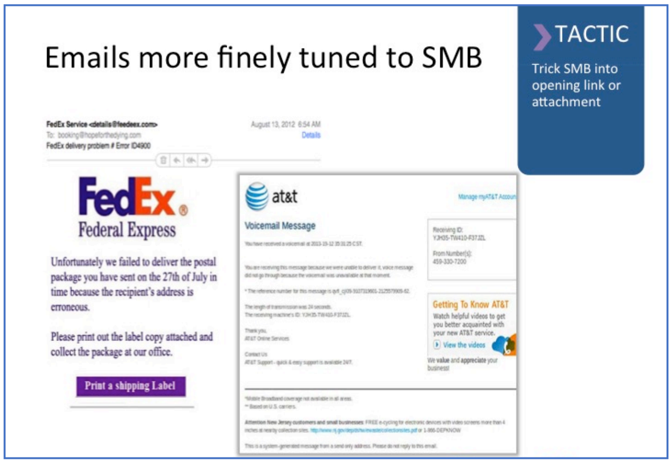
JACK THOMPSON

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.



Emails more finely tuned to SMB

TACTIC

Trick SMB into opening link or attachment

FedEx Service <details@feedeex.com>
To: booking@hopeforthedying.com
FedEx delivery problem # Error ID4900

August 13, 2012 6:54 AM
Details

FedEx Federal Express

Unfortunately we failed to deliver the postal package you have sent on the 27th of July in time because the recipient's address is erroneous.

Please print out the label copy attached and collect the package at our office.

Print a shipping Label

at&t

Manage myAT&T Account

Voicemail Message

You have received a voicemail at 2013-10-12 15:31:25 CST.

You are receiving this message because we were unable to deliver it, voice message did not go through because the voicemail was unavailable at that moment.

* The reference number for this message is qvt_cj09-9107319601-2125579909-62.

The length of transmission was 24 seconds.
The receiving machine's ID: YJH35-TW410-F37JZL.

Thank you,
AT&T Online Services

Contact Us
AT&T Support - quick & easy support is available 24/7.

Receiving ID:
YJH35-TW410-F37JZL

From Number(s):
459-330-7200

Getting To Know AT&T
Watch helpful videos to get you better acquainted with your new AT&T service.
View the videos

We value and appreciate your business!

*Mobile Broadband coverage not available in all areas.
** Based on U.S. carriers.

Attention New Jersey customers and small businesses: FREE e-cycling for electronic devices with video screens more than 4 inches at nearby collection sites. http://www.nj.gov/dep/dshw/ewaste/collectionsites.pdf or 1-866-DEPKNOW

This is a system-generated message from a send only address. Please do not reply to this email.

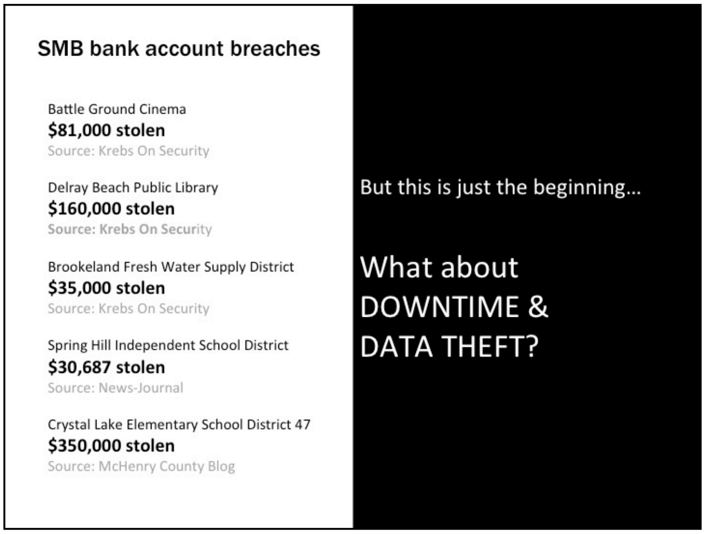
Recently I received notice that the $1,600 computer I ordered through Amazon had been shipped. It never happened. I figured it out when I noticed that the email came from Amazons.com, not Amazon.com. They were hoping I would click on a link that was enclosed. I didn’t.

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. My Amazons.com email had just such a link, but I knew to not open it.

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

If you are saying to yourself that you would never be fooled by this type of scheme, consider this: It doesn’t have to be YOU. If any one of your employees does falls victim to any of the above kinds of cyber-crime (and there are more that we have not mentioned), they could be opening up 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.



SMB bank account breaches

Battle Ground Cinema
$81,000 stolen
Source: Krebs On Security

Delray Beach Public Library
$160,000 stolen
Source: Krebs On Security

Brookeland Fresh Water Supply District
$35,000 stolen
Source: Krebs On Security

Spring Hill Independent School District
$30,687 stolen
Source: News-Journal

Crystal Lake Elementary School District 47
$350,000 stolen
Source: McHenry County Blog

But this is just the beginning…

What about DOWNTIME & DATA THEFT?

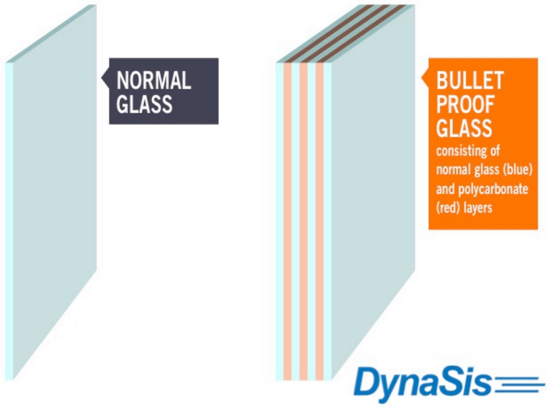
And here is something else of which to take note:

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

In last year's version of this paper, we discussed the 12 Layers of Protection that we at DynaSis use to safeguard our clients' networks. Just as cyber-attacks have taken giant steps forward in the past 12 months, so has cyber protection. Today, we begin with 12 layers and then offer a second set of layers we call **Security+**, based on a client's business and specific needs.

Security & Risk Mitigation: a Layered Approach


NORMAL GLASS
BULLET PROOF GLASS
consisting of normal glass (blue) and polycarbonate (red) layers
DynaSis

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 your IT service provider must 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.

This is best accomplished through a layered approach, which we equate to bullet-proof glass. The techniques described below were developed by a group of CEOs and Presidents of 12 independent IT service and security 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 thaYou must needs assistance.)

Some of these "layers" merit entire White Papers on their own, and much additional information is available in our weekly blog posts, (www.DynaSis.com/the-latest/) so please look at this analysis as an overview:

THE BASIC 12 LAYERS OF PROTECTION

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 Protection

You must stop threats at the gateway. Stops malware before it gets into the system. Blocks ZIP files. Provides sender authentication, recipient verification, message analysis, and spam rules.

Layer 3: Weekly Patch Updates

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

Layer 4: Anti-Malware

Anti-malware scans for malware and cleans it out. It looks for “zero-hour” malware and is regularly updated to identify latest versions. Performs daily in-depth scan of entire system.

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.

Layer 6: Firewall Port Lockdown

Signature based detection of viruses, intrusion protection. Allows only known inbound traffic (email, www, ftp) to pass. Configured for specific traffic to specific endpoints. Also locks down DNS requests from LAN to OpenDNS, preventing malware from using self-contained DNS resolution. Provides Virus ID and Geo filtering.

Layer 7: System Admin (Server Hardening)

Making sure that all best practices are followed, such as having event logs save the right types of data, seeing that their permissions are as they should be, and that people who have admin rights (and only those people) have them at the right level.

Layer 8: Cloud Delivered Predictive Security Service (Internet)

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: Strategic Technology Review (STR)

An in-depth review of all your technology from both a security and productivity point of view. It is designed to identify potential sources of weakness and quickly address these vulnerabilities before they become major problems.

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 or together potential failures. No level of security is 100% guaranteed, and effective backups provide the ability to restore data when locked or damaged.

SECURITY+

Since the introduction of the original 12 Layers of Protection, advances in cyber security technology have warranted the development of the next set of "layers" we call SECURITY+ and installed based on each client's needs, comfort level, and budget.

✚ **Security Assessment – Penetration Test**
From outside the network, we run an application that attempts to break through the firewall, and then reports its results.

✚ **Gateway Antivirus & Geo IP Filtering (Firewall)**
Additional protection to stop malware from getting into your system, and blocks outbound malware communication if it does. Can block email from whole countries/continents if your company is not doing business there.

✚ **Intrusion Protection**
Around the clock network protection that integrates a high- performance, deep packet inspection architecture with dynamically updated countermeasures for complete protection from application exploits and other malicious traffic

- **Email Security Protection – Mimecast**
  91% of hacking attacks begin with phishing or spear-phishing attacks. Even with training, 23% of phishing emails are opened, so protecting against human error is a top priority.

- **Multi-Factor Authentication (AD/RDS Servers)**
  Password related breaches are the leading cause of data loss. Data is protected by ensuring that only authorized people are given secure access to sensitive applications and information.

- **Removing Local User Admin Rights (User)**
  Reduces ability for malware to install itself and prevents employees from installing unauthorized software.

- **Security Awareness Training**
  As threats continue to evolve and grow, we provide ongoing training to your employees in the use of email, passwords, and other user-based vulnerabilities that hackers will exploit.

- **VPNs (Virtual Private Networks)**
  A VPN secures your computer's internet connection to guarantee that all the data you are sending and receiving is encrypted and secured from prying eyes.

- **MDM (Mobile Device Management)**
  In today's environment, companies must allow employees to use multiple types and brands of devices to remotely access corporate email, data and even applications. MDM gives you the control you need to maintain a high level of security.

- **Data Encryption**
  Content is encrypted as soon as it is created and synchronized encryption proactively protects your data by continuously validating the user, application, and security integrity of a device before allowing access to encrypted data.

- **SOC Services (Security Operations Network)**
  24 / 7 / 365 threat detection, remediation guidance, compliance, and SIEM and log management – all for a fraction of the cost of doing it yourself.

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, such an assessment can be very helpful and the upgrades it may point to, because it will enable your team to better sleep at night (you, too!) and be more productive at their jobs. It is not the goal of a good managed IT service and security 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.

Check our weekly blog posts at: www.DynaSis.com/The-Latest