Ransomware:
To Pay or Not To Pay?

That should never be the question.

esentire®

What is Ransomware?

Ransomware is crippling organizations across industries. Its overwhelming effectiveness has made it an attack method of choice for cybercriminals.

Ransomware has become so popular that it now has its own evolutionary tree with names like TESLECRYPT, ZEPTPO and LOCKY. Continual evolution is what helps its variants evade the security defenses working to detect them.

There are two distinct variants of ransomware: crypto and locker. Crypto encrypts files, folders and hard drives. Locker locks out users of their devices. According to the FBI, ransomware attacks made $209 million in the first quarter of 2016[1]. They predict that number will exceed $1 billion by the end of the year[2].

[1] http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/
[2] https://www.esentire.com/blog/ddos-2-0-is-ransomware-the-next-evolution-of-ddos/

Why is Ransomware so Prevalent?

It's easy.

It isn't difficult to understand why ransomware is an appealing method to many cybercriminals. Compared to traditional attack methods, with ransomware, criminals can achieve payment with fewer steps resulting in a more direct route to payment.

Publically available toolkits have also made it easy for would-be cybercriminals to develop effective ransomware. Today's reality is that ransomware-as-a-service can even be purchased on the dark web.

It's lucrative.

Cybercrime is a lucrative business and the financial gain is a significant driver in the evolution of what malicious software is to come. It's safe to say that ransomware will continue to evolve and infect more devices in the years to come[3].

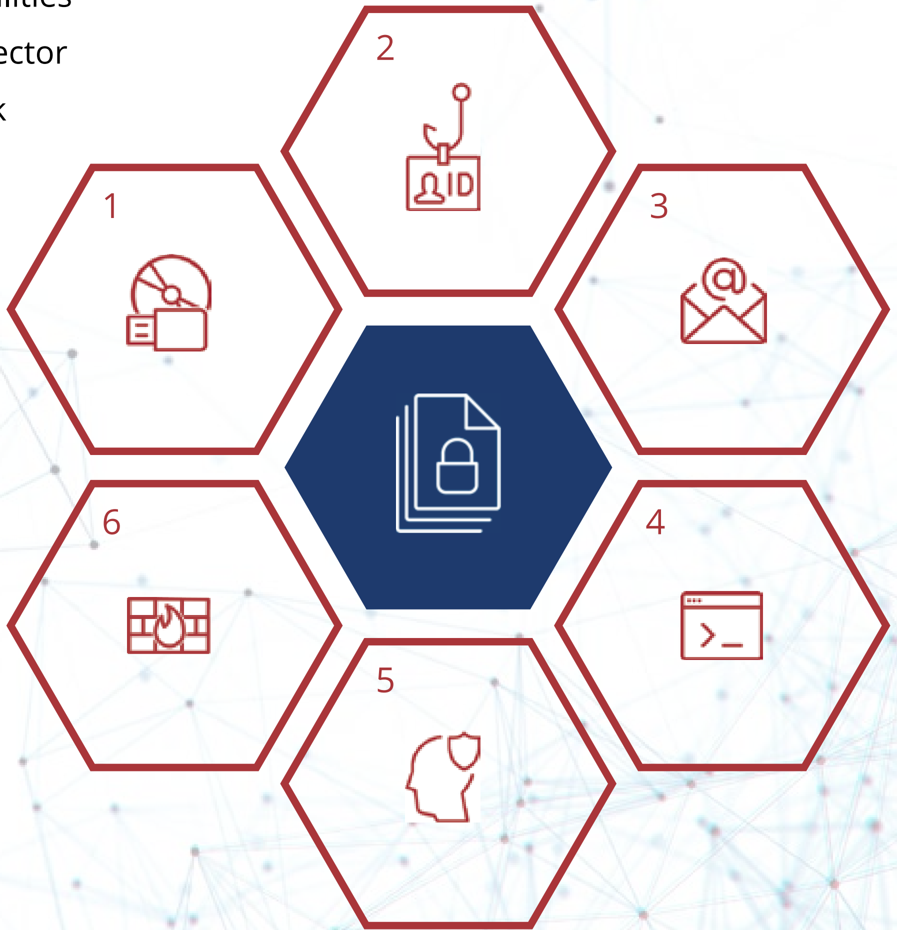
Businesses aren't prepared.

Attacks targeting mid-sized businesses have been particularly effective. Organizations lacking adequate system back-ups have resorted to meeting ransom demands to reclaim critical business files. Unfortunately, in many cases paying the ransom does not guarantee that the victim will be able to fully restore encrypted files.

[3] https://www.esentire.com/news-and-events/coverage/q1-2016-saw-a-record-high-for-ransomware/

How Does Ransomware Infiltrate Your Network?

1. Infected Media
2. Phishing / Malicious Links
3. Phishing / Malicious Attachments
4. Web Application Vulnerabilities
5. New Variant / Unknown Vector
6. Brute Force Firewall Attack



What is the Risk of Ransomware?

- Temporary or permanent loss of mission critical, confidential or proprietary information
- Possible loss of data through exfiltration
- Financial losses including ransom payment, investigation, system remediation, and lost billable hours
- Disruption of regular operations
- Harm to the firm's reputation, associated with disruption of service and/or public awareness of a breach
- Fines levied by regulatory organizations

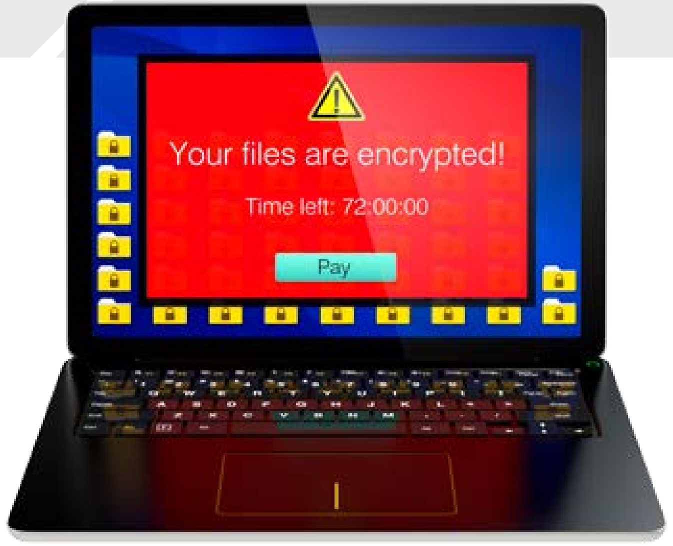
To Pay or Not to Pay: What Are Your Options?

PAY

the ransom

DON'T PAY

and recover from back-up files



How Can You Protect Your Firm?

Human Defense Mechanisms

Minimum

- Train staff to help with the proactive detection of malicious content
- Conduct annual employee phishing tests
- Create Incident Response plans

Intermediate

- Preform monthly phishing testing
- Preform quarterly review of incident response plans
- Investigate a continuous monitoring/embedded incident response methodology

Advanced

- Preform daily micro-training

Upstream/Local Email Provider Defense Mechanisms

Minimum

- Block content based on executables
- Block content based on file suffix
- Isolate/sandbox inbound attachments based on content

Intermediate

- Scan/MD5 all attachments and compare
- Block content based on known bad actors
- Whitelist known senders of malicious attachments
- Scan all embedded URLs
- Employ PTR/Sender Policy Framework (SPF) for anti-spoofing protection

Advanced

- Sandbox all attachments
- Enforce the transfer of files through means other than email

General Services Within Information Technology

Minimum

- Backup all critical systems
- Test restore process quarterly
- Enforce patch rigor on fileservers
- Restrict access to critical data through selective privileges
- Restrict access to personal email

Intermediate

- Backup all critical systems with frequent snapshots sent offsite
- Backup critical workstation components
- Test restore processes monthly
- Enable a methodology to alert when a single user modifies multiple files within a short, specific period of time

Advanced

- Preform regular backups of critical mobile devices
- Investigate the use of File System Resource Manager (FSRM) to block the creation of file with known ransomware suffixes

Network-Focused Security Components

Minimum

- Investigate malware defense options within existing firewall
- Blacklist known bad IP addresses

Intermediate

- Block blacklisted command and control channels
- Enable geo-blocking of blacklisted countries
- Block Adobe Flash execution at the firewall level
- Consider sandboxing of traffic recently-created domains
- Blacklist known bad domains within Domain Name System (DNS)
- Blacklist known bad websites through web proxy capabilities
- Greylist recently-created domains through web proxy capabilities

Advanced

- Block blacklisted/whitelisted content at the firewall level
- Blacklist Demand Generation Algorithms (DGA) domains within Domain Name System (DNS)

Endpoint Protection Measures

Minimum

- Standardize regularly-patch operating systems
- Use established and effective anti-virus solutions
- Ensure Microsoft Office suite is up-to-date
- Disable macro usage within Microsoft Office
- Ensure browsers are trusted, up-to-date and regularly patched

Intermediate

- Use the Microsoft Viewer Suite instead of the full Microsoft Office Suite
- Disable Adobe Flash where possible
- Disable PowerShell where possible
- Enable Microsoft defense tools, such a AppLocker and Enhanced Mitigation Experience Toolkit (EMET)

Advanced

- Investigate next-generation antivirus solutions
- Investigate additional endpoint defense tools including MBR Filter

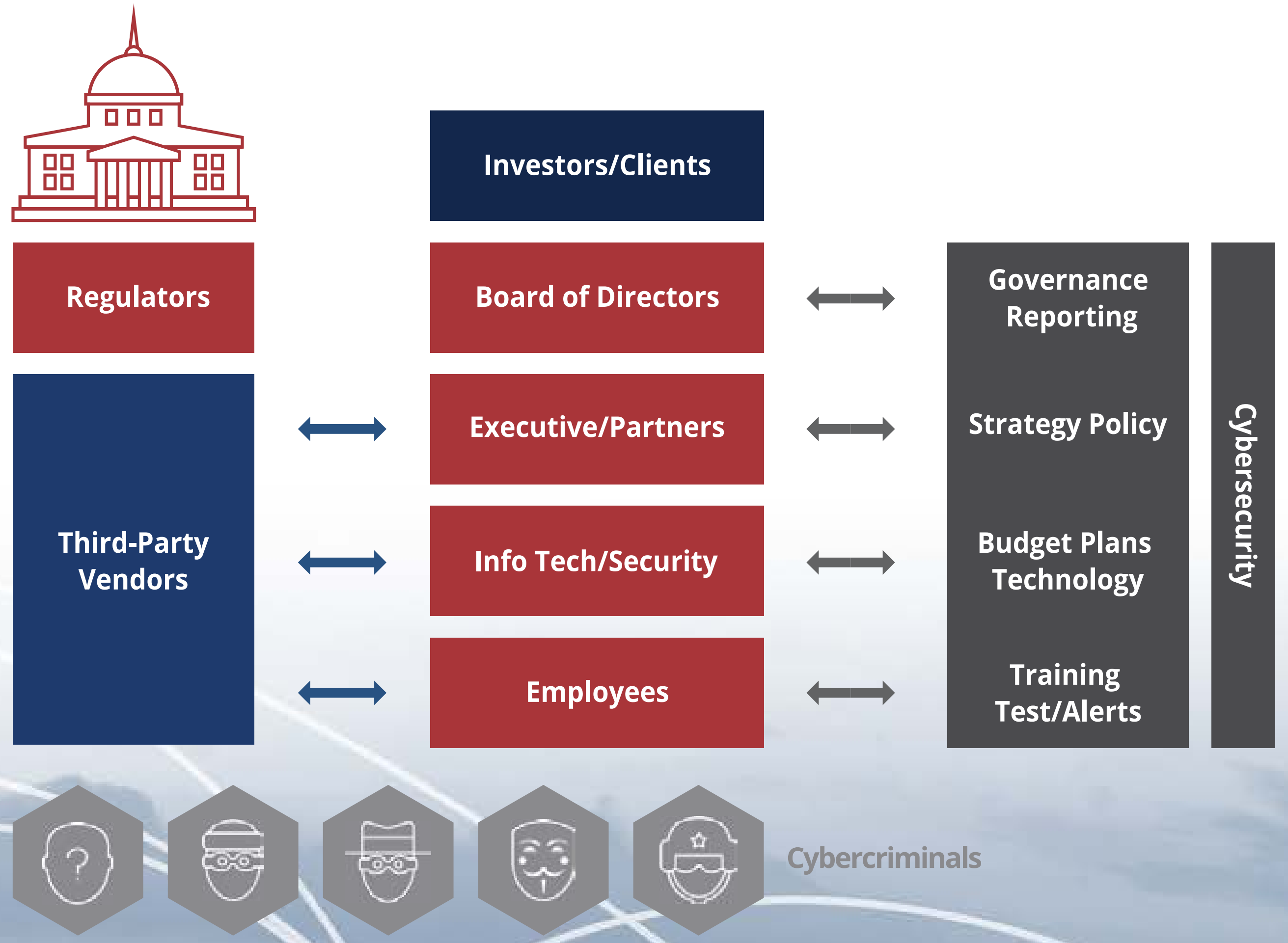
Ransomware is on Everyone's Mind

It's not just IT's problem.

The increase in the number of ransomware attacks and their growing effectiveness in crippling your business requires prevention at the core of your cybersecurity policy. Ransomware demonstrates that the responsibility for cybersecurity practices are not limited to the information technology team or even the security team. Every level of your organization plays a role in protecting your networks against cyber-attacks.

Third parties could be the weak link.

A lot of firms see third-party service vendors as an extension of their organization. What many don't realize is these third-party vendors can be your weakest security link. When looking into third-party vendors it's important to ask if their cybersecurity posture is up-to-date.



Regulators

Investors/Clients

Board of Directors

Executive/Partners

Info Tech/Security

Employees

Third-Party Vendors

Governance Reporting

Strategy Policy

Budget Plans Technology

Training Test/Alerts

Cybersecurity

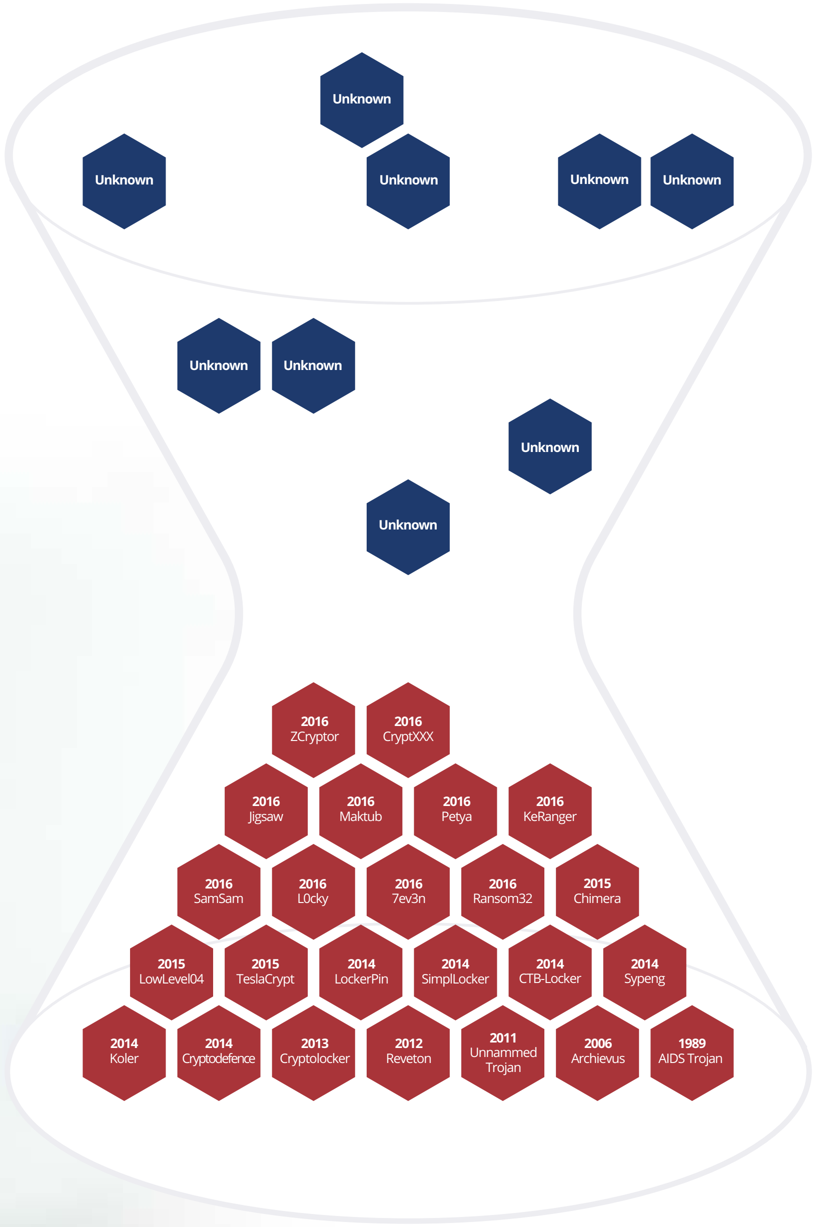
Cybercriminals

The Evolution of Ransomware

There have been dozens of known ransomware attacks over the past few decades. Year-over-year, the number of variants continues to multiply, threatening to disrupt the livelihood of your business.

Cybersecurity solutions have evolved to include signatures to prevent these known variants. With this in mind, one question remains: **what about the unknown?**

Traditional technologies alone cannot catch unknown cyber threats. These threats are unique; your cybersecurity defenses should be to. Human monitoring and hunting is critical to your cybersecurity providers' ability to catch new variants. It's important to review how your cybersecurity provider detects these unknown threats.



Unknown

Unknown

Unknown

Unknown

Unknown

Unknown

Unknown

Unknown

Unknown

2016 ZCryptor

2016 CryptXXX

2016 Jigsaw

2016 Maktub

2016 Petya

2016 KeRanger

2016 SamSam

2016 L0cky

2016 7ev3n

2016 Ransom32

2015 Chimera

2015 LowLevel04

2015 TeslaCrypt

2014 LockerPin

2014 SimplLocker

2014 CTB-Locker

2014 Sypeng

2014 Koler

2014 Cryptodefence

2013 Cryptolocker

2012 Reveton

2011 Unnammed Trojan

2006 Archievus

1989 AIDS Trojan

We Can Help

eSentire Managed Detection and Response™ keeps organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Our 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates and responds in real-time to known and unknown threats before they become business disrupting events.

eSentire absorbs the complexity of cybersecurity providing enterprise-class protection to protect against advanced cyber-attacks. Visit www.eSentire.com to learn why managed detection and response is the best way to protect your business from the growing threat of ransomware.

Malware evolution seems to be as rapid and cutthroat as any jungle environment, where survival and propagation go hand in hand. Authors have frequently co-opted functionality from different malware strains into the next generation of code — regularly sampling the efficacy and profitability of each generation.

– Eldon Sprickerhoff,
eSentire Founder and Chief
Security Strategist

esentire®

About eSentire

eSentire® is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business disrupting events. Protecting more than $5 trillion in corporate assets, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements.

For more information, visit www.eSentire.com and follow @eSentire.