

AlphaKOR Ransomware Defense

Follow us on Twitter: [@AlphaKOR](https://twitter.com/AlphaKOR)

Visit our Blog:

www.AlphaKOR.com/blog

The Facts of the Presentation

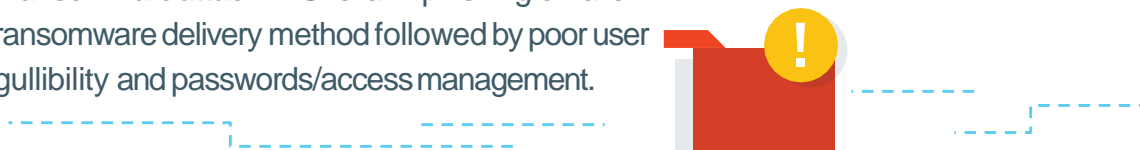
The 2019 AlphaKOR Ransomware Report is comprised of statistics pulled from a survey of over 2500 managed service providers (MSPs), like AlphaKOR, across the US & Canada with survey data extracted to show Canadian only responses.

The report provides unique visibility into the state of ransomware from the perspective of the business owners and IT Professionals who are dealing with these infections on a daily basis. The report provides a wealth of detail on ransomware, including year-over-year trends, frequency, targets, impact, and recommendations for ensuring recovery and business continuity in the face of the growing threat.

Key Findings



- **Ransomware remains a massive threat to small-to-mid-sized businesses (SMBs).** From Q2 2016 - Q2 2018, 83% of SMBs reported ransomware attacks against their infrastructure. In the first 6 months of 2018 alone, 55% reported increase of ransomware attacks compared to the previous year. 92% of MSPs predict the number of ransomware attacks will continue at current, or worse, rates based on poor client education and a continued security by obscurity mindset.
- **The average managed service providers (MSPs) report 4 of these attacks within their client base per year.** In the first half of 2018, an alarming 37 of MSPs report clients suffered multiple attacks in a single day (up from 31 from 2017).
- **There is mandatory reporting in place.** PIPEDA legislation requires that RROSH breaches are reported to clients and authorities https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/
- **SMBs are largely in the dark about the frequency and severity of ransomware attacks.** Nearly 90 of MSPs are “highly concerned” about the ransomware threat and 33 report their SMB clients feel the same.
- **Lack of cybersecurity education is a leading cause of a successful ransomware attack.** MSPs rank phishing emails as the top ransomware delivery method followed by poor user practices/gullibility and passwords/access management.
- **The aftermath of a ransomware attack can be crippling for a business.** When asked about the impacts of a successful attack, 70 of MSPs report victimized clients experienced a loss of business productivity. More than half report clients experienced business-threatening downtime.
- **The cost of business downtime is 7.5X greater than the cost of the ransom requested.** Canada not only has the highest average cost of ransom, but also the highest cost of downtime globally. MSPs report the average requested ransom for SMBs is ~\$8,764 CAD while the average cost of downtime related to a ransomware attack is ~\$65,724 CAD.
- **Canadian SMBs report Windows as the most targeted system by hackers.** They are also seeing a rise in attacks on Apple and Android systems.
- **Ransomware infections in the cloud continue to increase year-over-year.** Of MSPs that report cloud-based malware infections, nearly 50 called out Office 365 as the target.
- **In comparison to other solutions, the most effective for avoiding downtime caused by ransomware is business continuity and disaster recovery.** Roughly 90% of SMBs victimized clients with BCDR in place fully recovered from the attack in 24 hours, or less.



Ransomware Most Prominent Malware Threat to SMBs

List of US and Canada client-based attacks against SMB's in the last 2 years

(Cisco Umbrella Analytics for Canada 2018)

83% reporting clients struck by ransomware

65% reporting clients struck by viruses

56% reporting clients struck by spyware

54% reporting clients struck by adware

39% reporting clients struck by trojan horses

24% reporting clients struck by cryptojacking

24% reporting clients struck by rootkits

19% reporting clients struck by worms

18% reporting clients struck by keyloggers



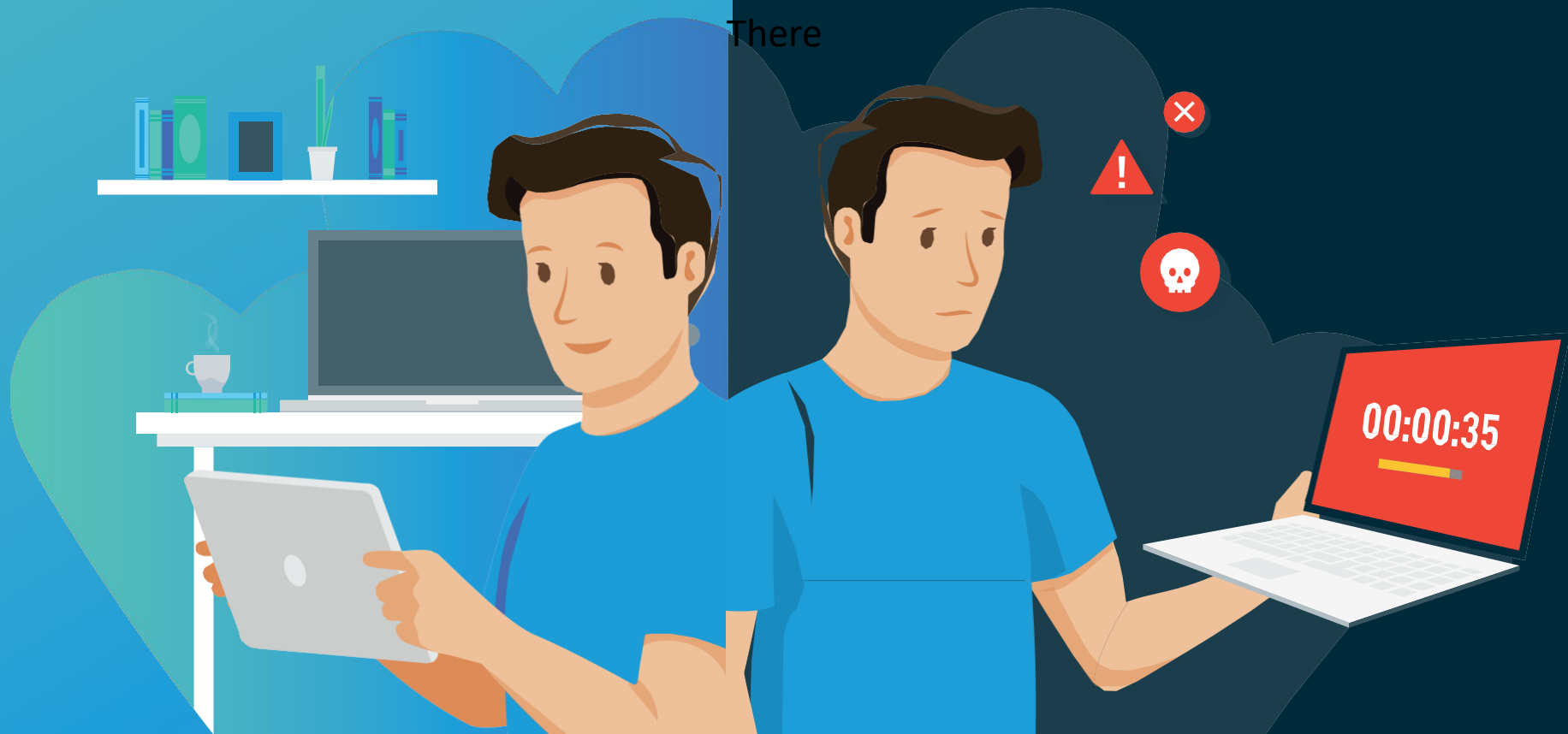
Most SMBs Unaware of Ransomware Risk

Only 33% of SMBs
report they are “highly
concerned” about ransomware.

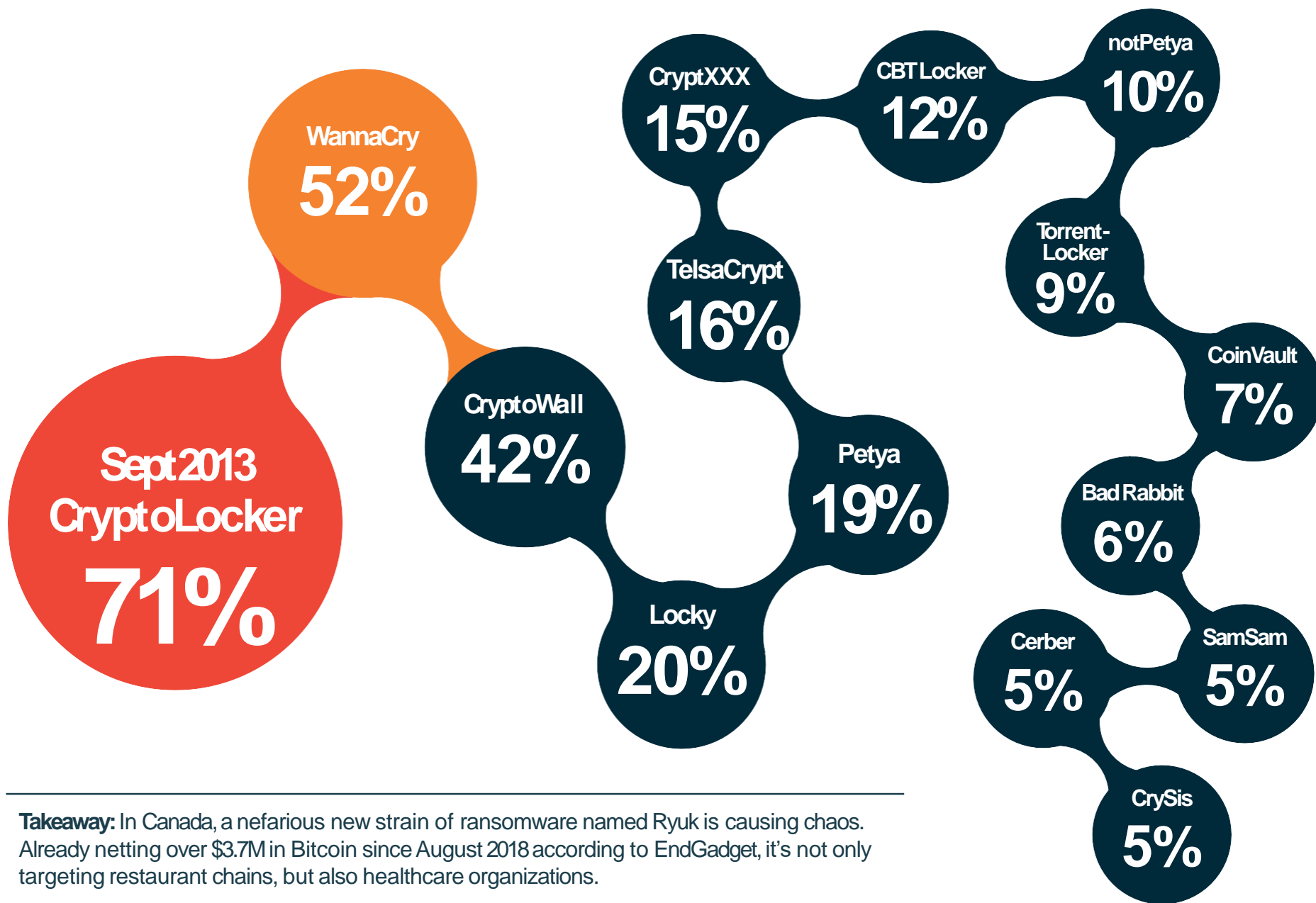
According to a 2019 vendor study of Canadian SMB's

90% of MSPs
think they should be.

Here's why...



CryptoLocker and WannaCry Reign Supreme



End User Error is the Common Denominator

Top Ransomware Delivery Methods:

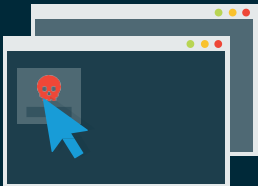


80% of SMBs

Report Phishing
Emails

25% of
SMBs
Report Clickbait

You Won't Believe...



23% of
SMBs

Report Malicious
Websites/Web Ads

Top Cybersecurity Vulnerabilities:

View Attachments



32% of
SMBs

Report Poor User
Practices/Gullibility

29% of
MSPs

Report Lack of End User
Cybersecurity Training



29% of SMBs

Report Weak
Passwords/Access
Management

I * * * * *

 Reply  Reply All  Forward

Mon 2019-05-13 2:56 PM



IT <IT@alphakor.com>

Urgent: Mandatory Password Reset

 Daniel Charnock



Action Items

+ Get more add-ins



Your IT administrator has initiated a mandatory password reset for your organization due to a suspected hacking attempt.

Please create a new password immediately to ensure your account is protected.

[CREATE NEW PASSWORD](#)

© Microsoft Team. All rights reserved.

Reply Reply All Forward

Mon 2019-05-13 2:56 PM



IT <IT@alphakor.com> it@alphakor.sentex.ru



Urgent: Mandatory Password Reset

To Daniel Charnock



Action Items

+ Get more add-ins



Your IT administrator has initiated a mandatory password reset for you due to a suspected hacking attempt.

Please create a new password immediately to ensure your account remains secure.

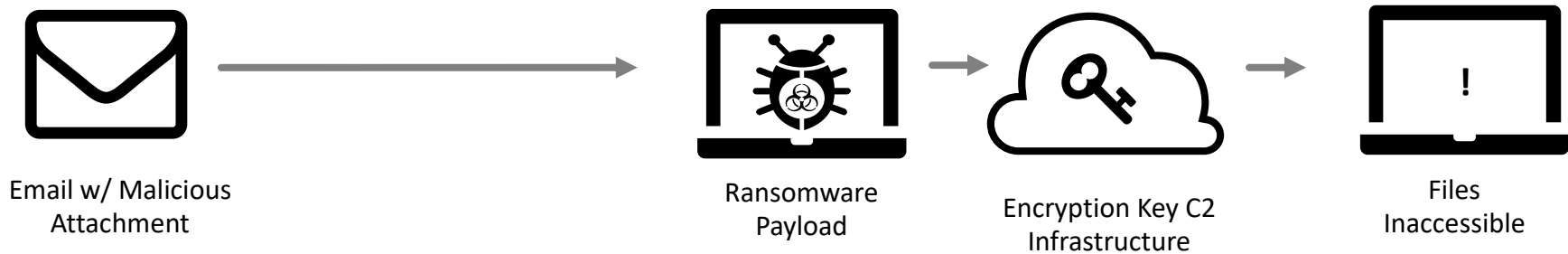
<http://cardpayments.microransom.us/xcmvfjaxbpzwq50x2lkptjq1ntg2nlodyzmoczjyw1waywllnb19ydw5fawq9mjayvmzy1nszhy3rpb249y2xpy2smdxjspwh0dhbzoi8vc2vjdxjlzc1sb2dpbi5uzxqvcgfnxmvnwi2ztjkodc5njfi>
Click or tap to follow link.

[CREATE NEW PASSWORD](#)

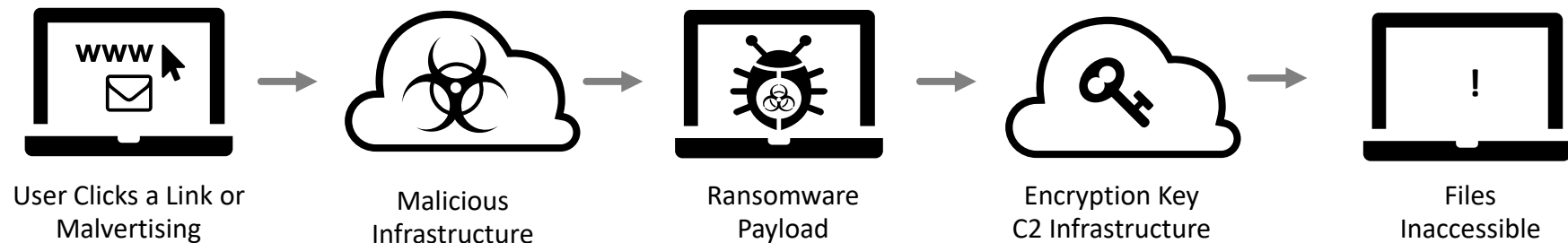
© Microsoft Team. All rights reserved.

How Ransomware Works

EMAIL-BASED INFECTION



WEB-BASED INFECTION

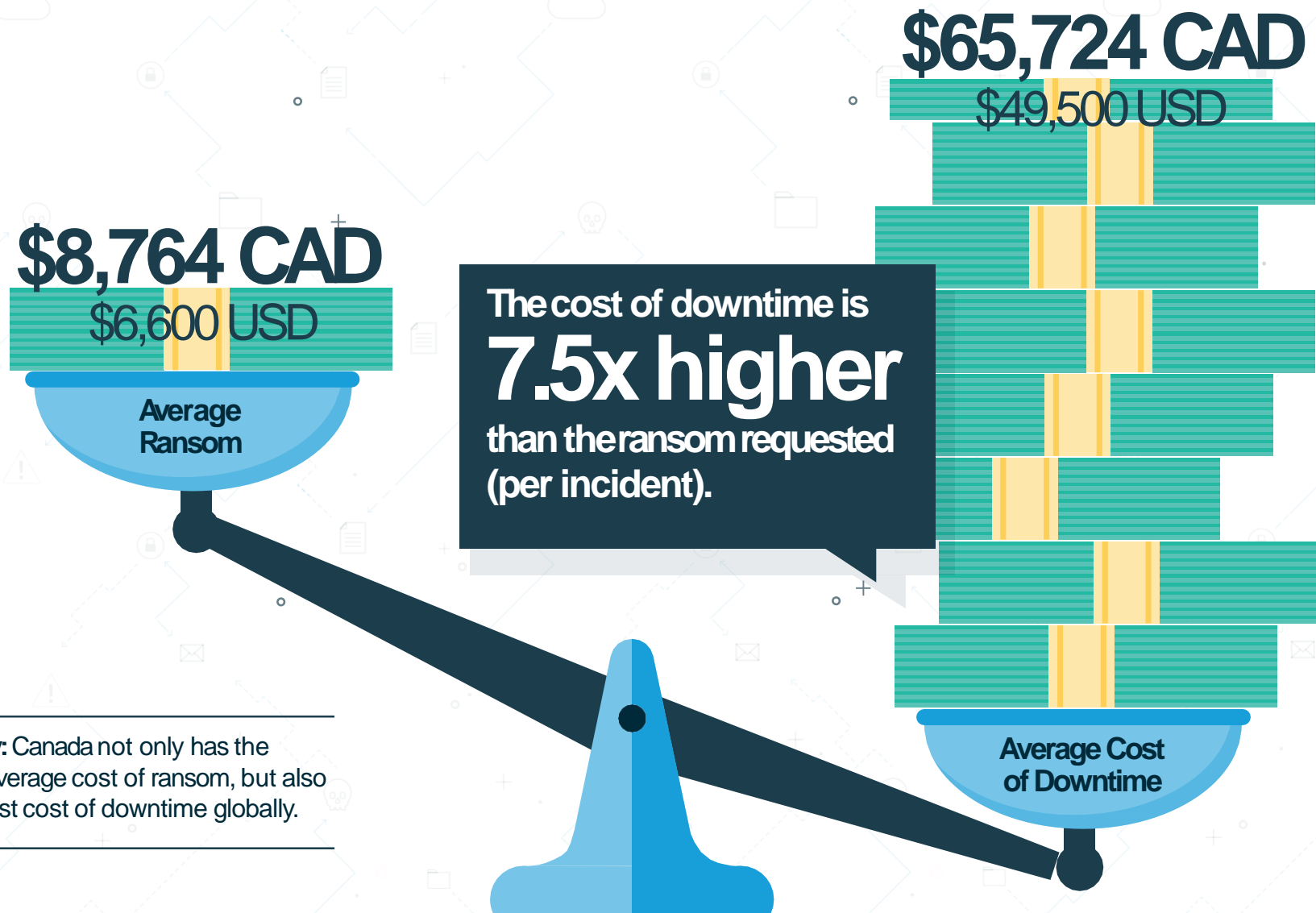


Quebec Region Immobilized by Ransomware Attack

The regional municipality of Mekinac in Quebec fell victim to a CryptoLocker ransomware attack in September, 2018. Mekinac's servers were compromised after an employee opened and clicked on a link in a fraudulent email sent by the hackers. For two weeks, servers were disabled and employees were unable to work. The attack not only impacted government employees, but also affected 10 municipalities with a population of roughly 13,000 people.



Cost of Downtime Significantly Outweighs Ransom Requested



Takeaway: Canada not only has the highest average cost of ransom, but also the highest cost of downtime globally.

1USD = 1.33CAD per conversion rates in May 2019.

*Cisco survey respondents of companies consisting of 50 or less employees. Answers in U.S. dollars.

Ransomware Attacks Are Costly

Survey of SMB ownership experiences following a successful ransomware attack
(Geo Trend Canadian Survey 2018)

70% reported loss of business productivity

57% reported business-threatening downtime

42% reported significant data loss

41% reported infection spread to other devices on the network

31% reported a loss of yearly profitability

31% paid a ransom and recovered the data

29% reported amaged reputations

18% reported stolen data

17% reported ransomware remained on systems, struck again!

14% reported IT staff failed to respond to adequately to the attack

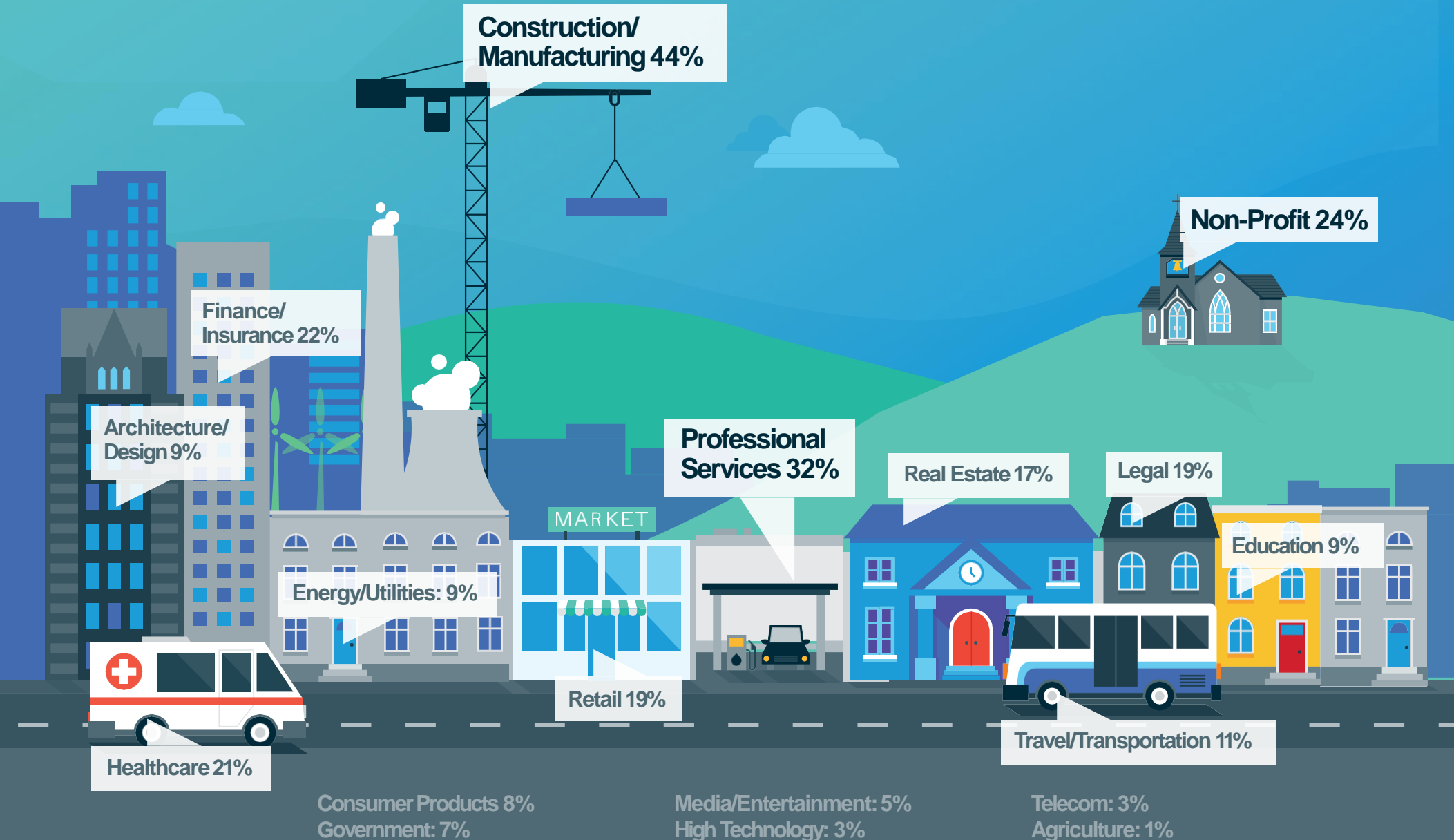
9% paid a ransom, data was never released

8% reported failure to achieve regulatory compliance



No Industry is Safe from Ransomware

Industries victimized by ransomware



Ransomware Will Creep into the Cloud

24% of MSPs have seen ransomware attacks in SaaS applications (up 2% from last year)

Of the 24% :

 Office 365

**56% Report
O365 Infections
(up 34% from last year)**

 Suite

**25% Report
GSuite Infections
(up 17% from last year)**

Geo Trend: Globally in 2019, 28% of MSPs reported ransomware infections in cloud-based applications vs 24% in Canada.

SMBs Report Windows as Most Targeted System by Ransomware

80%
Windows



11%
3% 2017
macOS



5%
Android

iOS

4%
iOS

Takeaway: Mac ransomware attacks are growing. The number of MSPs reporting OS attacks increased by 8% from 2017 to 2018.

No One System Can Entirely Prevent Ransomware



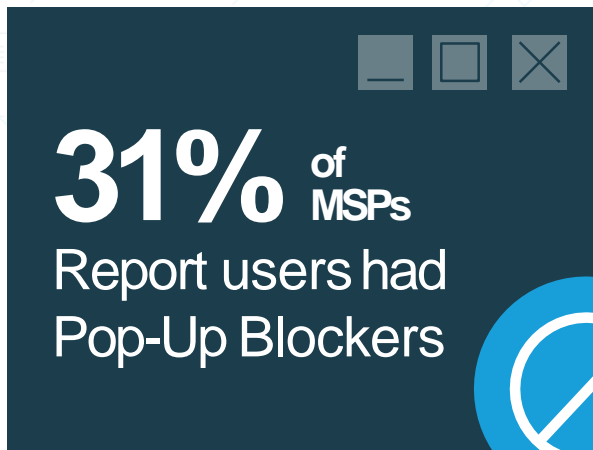
85% of
SMBs

Report users had
Antivirus Installed



69% of
SMBs

Report users had
Email/Spam Filters



31% of
MSPs

Report users had
Pop-Up Blockers

Takeaway: As no single solution is guaranteed to prevent ransomware attacks, a multilayered portfolio is highly recommended.

The Five Most Effective solutions for Ransomware

#1 Firewall or Unified Threat Management Equipment

#2 Antivirus/Malware

#3 Business Continuity/Disaster Recovery

#4 Patch Management

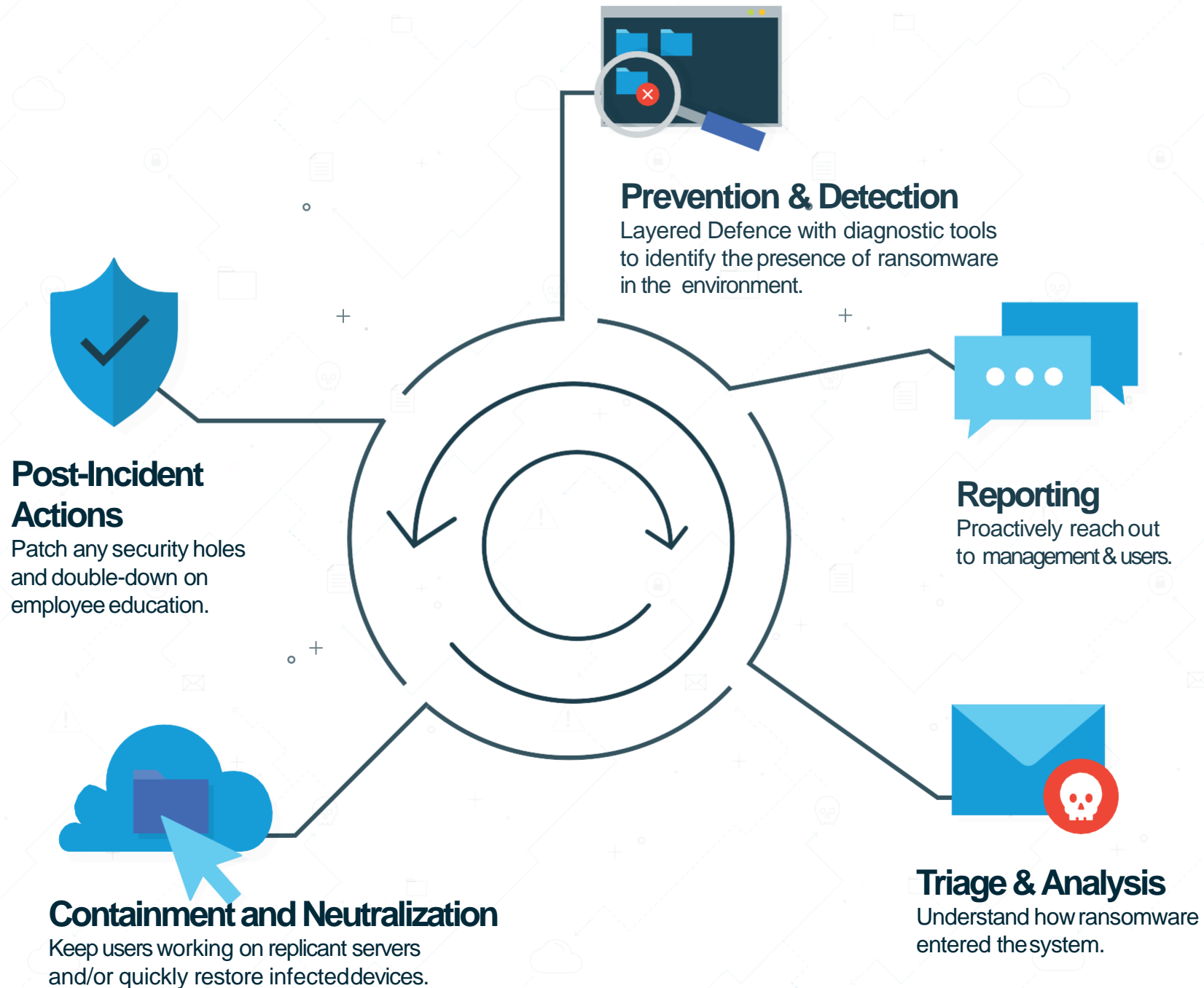
#5 Employee and Executive Training

Takeaway: Ransomware attacks will inevitably happen. To protect clients and effectively respond to attacks, BCDR and UTM is crucial to prevent downtime.

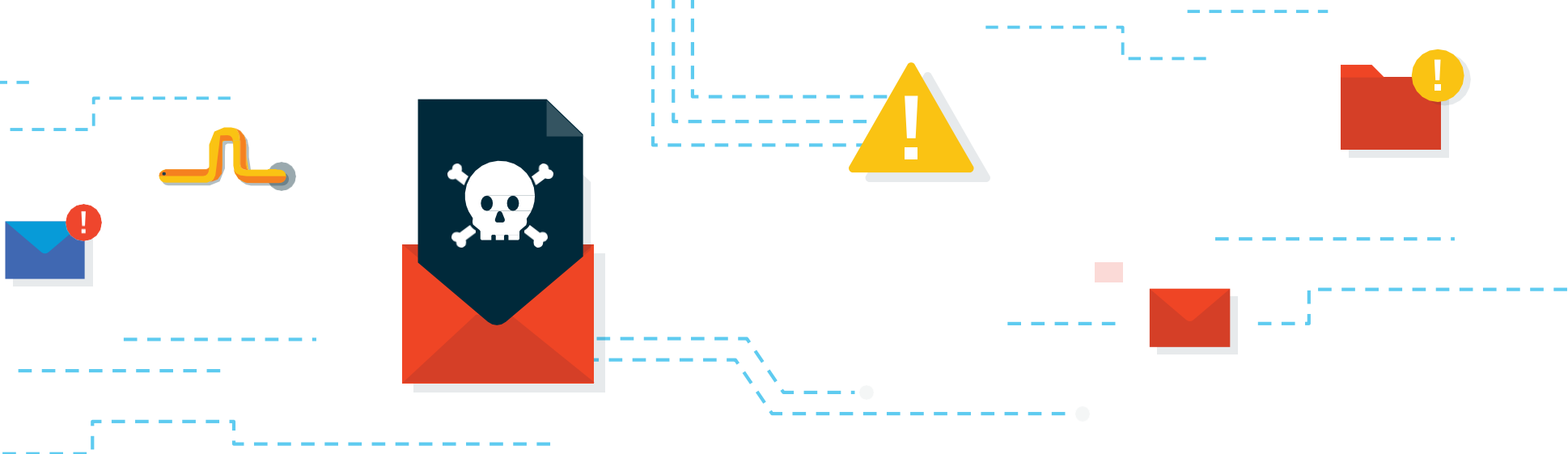
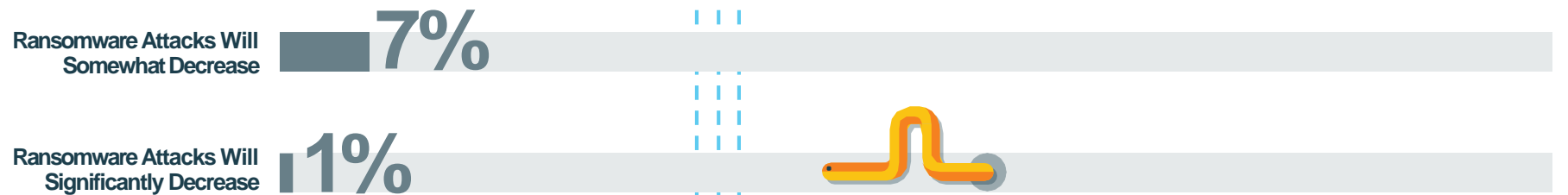
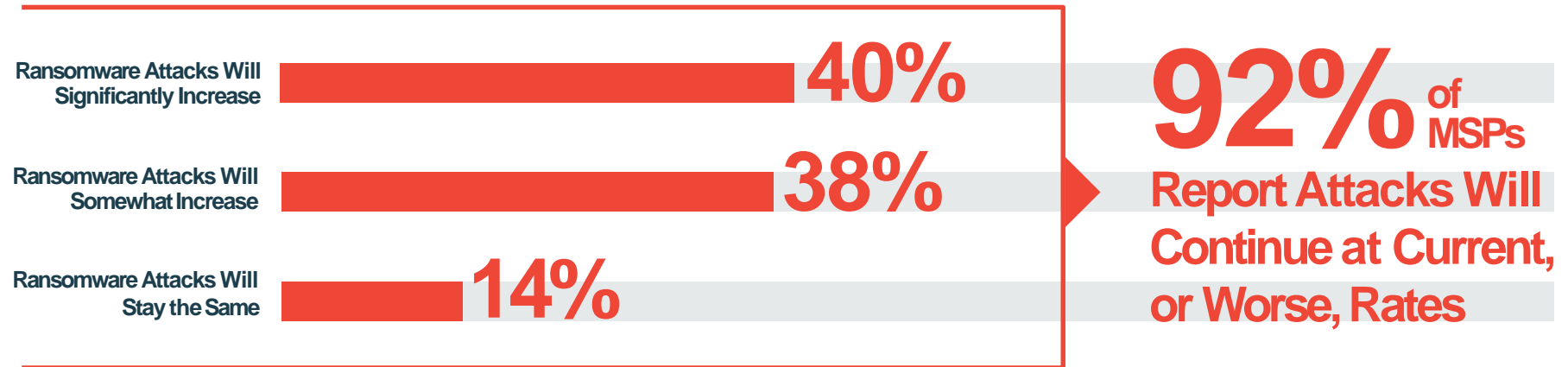
*BCDR: Business Continuity and Disaster Recovery

*UTM – Universal Threat Management

A Typical Ransomware Response Plan starts with Preparation

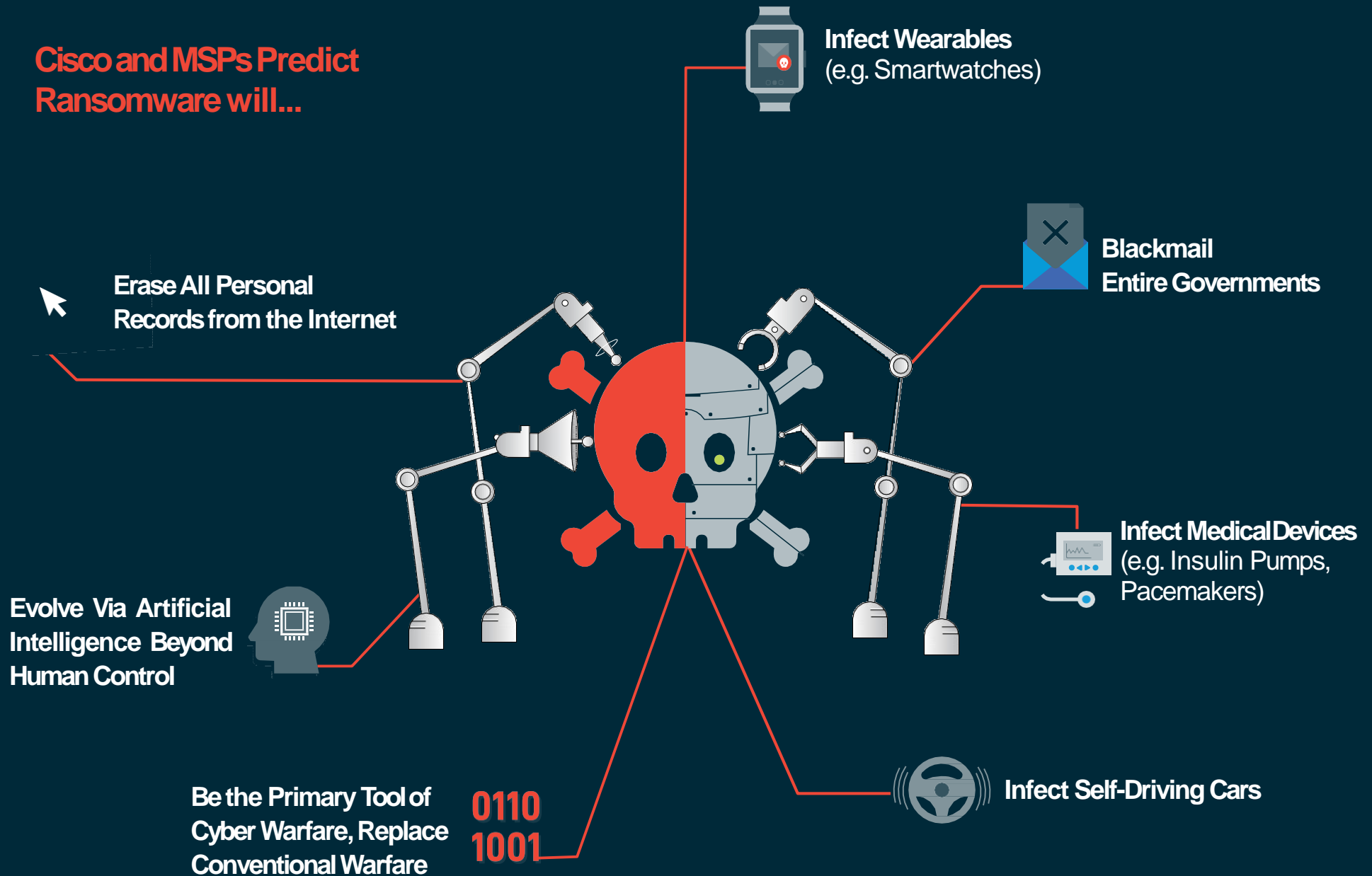


Majority of MSPs Report: Ransomware is Here to Stay



Ransomware Will Wreak Havoc Everywhere

Cisco and MSPs Predict Ransomware will...



Ransomware of the Future Gets Personal



60% of MSPs

Predict Ransomware Will Target
Social Media Accounts



59% of MSPs

Predict Ransomware Will Target
IoT Devices



53% of MSPs

Predict Ransomware Will Target &
Bankrupt Entire Companies



47% of MSPs

Predict Ransomware Will Target
Critical Utilities Infrastructures

(e.g. Power Grids)

<https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110>



37% of MSPs

Predict Ransomware Will Target
Users Based On Personal Attributes

(e.g. Race, Religion, Political Views)

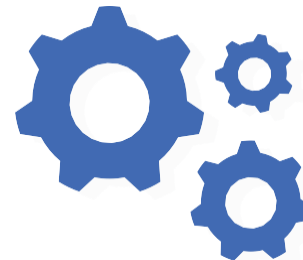
Final Takeaways



Businesses must prepare the front line of defense: your employees. Today's companies must provide regular and mandatory cybersecurity training to ensure all employees are able to spot and avoid a potential phishing scam in their inbox, a leading entrance point for ransomware.



Businesses must leverage multiple solutions to prepare for the worst. Today's standard security solutions are no match for today's ransomware, which can penetrate organizations in multiple ways. Reducing the risk of infections requires a multilayered approach rather than a single product.



Businesses must ensure BCDR and Threat Management is in place. There is no sure fire way of preventing ransomware. Instead, businesses should focus on how to maintain operations despite a ransomware attack or infection. One way to do this is a layered threat management system and a reliable business continuity and disaster recovery solution.



Businesses need a dedicated cybersecurity professional to ensure business continuity. SMBs often rely on a "computer savvy" staff member to handle their IT support and not an IT expert. If a company cannot afford a complete IT staff for 24/7 cybersecurity monitoring, they should be leveraging a Managed Service Provider (MSP) who has the time and resources to anticipate and protect a company from the latest cybersecurity threats.