



ASMGi

ONEteam

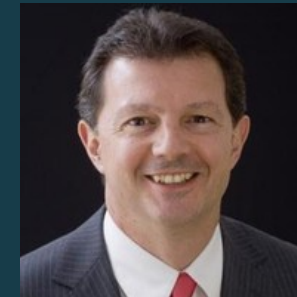
The Real Cost of Ransomware and Rethinking your DR

October 15, 2020

The Real Cost of Ransomware and Rethinking your DR



Frank Yako
CIO, Director of Strategic Initiatives
ASMGi



Steve Roesing
President, CEO
ASMGi

ASMGi is full-stack technology company headquartered in Cleveland, OH. Our expertise across the full spectrum of IT Services, GRC & Cyber Services and SDLC Services enables our *X as a Service* model to deliver value to our customers.



ONEteam

Agenda

- ◆ *Introduction*
- ◆ *What is the Cost of Ransomware?*
- ◆ *How does Ransomware happen?*
- ◆ *How to **Prevent Ransomware** and/or **Recover from Ransomware***
- ◆ *Summary & Key Takeaways*
- ◆ *Q & A*

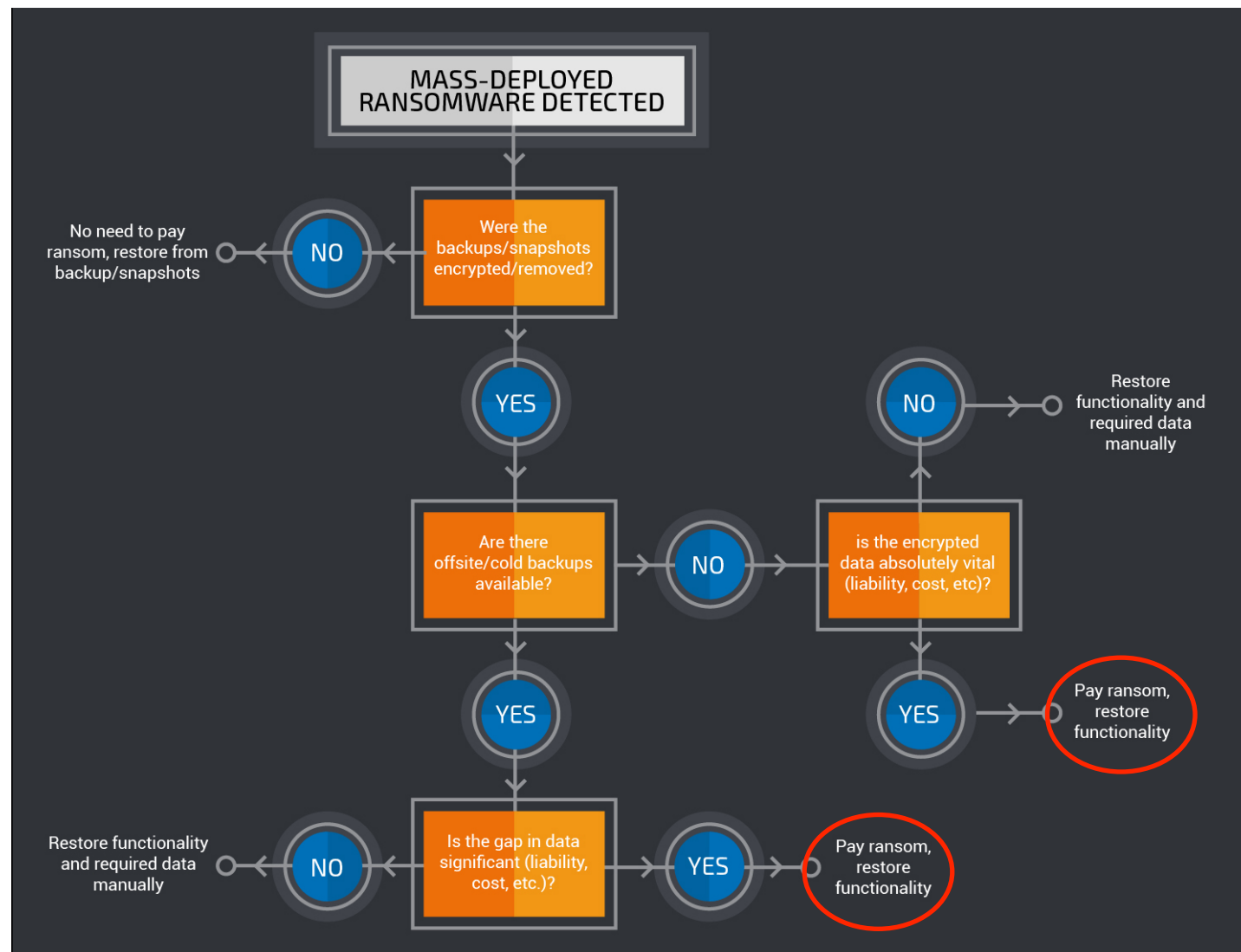
2020 is the year of Ransomware



“2020 is the year of Ransomware. We will see a spike in attacks and in successful attacks. Ransomware is the most direct path for attackers to make money, and lots of it. Fundamentally, while I think paying the ransom is a bad idea, I’ve come to realize that paying the ransom or not paying the ransom is a business decision. Our jobs are to never put people in the position that their best business decision is to pay the ransom.”

Steve Roesing, ASMGi

2020 is the year of Ransomware



What is the Real Cost of Ransomware?

UHS hospital chain hit with apparent ransomware attack

Universal Health Services, which operates about 400 facilities, was targeted with a cyberattack over the weekend that has triggered a multiday IT outage.

THE LARGER TREND

Ransomware attacks can prove dangerous – even deadly – for patients. Earlier this month, a [German woman died](#) after a ransomware attack necessitated a move between hospitals. It is said to be the first fatality linked to a ransomware attack.

As the security professionals noted, the COVID-19 pandemic has facilitated opportunities for cybercriminals, with many employees working from home and IT systems undergoing [rapid, often large](#), changes.

"Any time you make a change to an IT environment, you have the potential to increase risk," said Andy Riley, executive director of security strategy at the managed-security-services vendor Nuspire, in an interview this summer.

2020 is the year of Ransomware

So what can we expect in 2020 and beyond? Here are a few predictions.

- Cybersecurity Ventures predicts ransomware will cost \$6 trillion annually by 2021. (Source: [Cybersecurity Ventures](#))
- McAfee predicts some common ransomware targets will decrease. However, the company suggests cybercriminals will target less common and more vulnerable victims, such as individuals with high net values and connected devices (IoT). (Source: [McAfee](#))
- Palo Alto Networks predicts a noticeable increase in Mac ransomware. (Source: [Palo Alto Networks](#))
- MIT predicts cloud computing companies will see increased attacks against their systems. (Source: [Computer Weekly](#))
- According to RSA Security, the future of this growing threat will include not just a lockdown on integral files and folders, but access to networks and accounts. (Source: [RSA Security](#))

2020 is the year of Ransomware



The biggest news-maker for 2019, in fact, is the Baltimore City government. The city's computer system was hit with a ransomware infection in May 2019 that kept the city's government crippled for over a month. Estimates put the cost to recover at [over \\$18 million dollars](#), although the cybercriminal behind the malware only demanded \$76,000 worth of Bitcoin. The attack reportedly impacted vaccine production, ATMs, airports, and hospitals.

Just about a year earlier, the [Atlanta city government](#) spent over \$17 million to recover from a virus attack that demanded \$52,000 in Bitcoin.

While many chose not to pay the cost for ransomware (and indeed, most security professionals say paying is typically a [bad idea anyway](#)), those that do pay up often find their files remain encrypted. After all, placing trust in the good graces of criminals is often leads to disappointment.

2020 is the year of Ransomware



The most interesting data is to see how cybercriminals ask for and are able to get varying sums of money for the decryption key. According to the report:

- The average payout for school districts (Education) was \$132K
- The average for higher education was \$154K
- Manufacturing averaged a payment of \$172K
- Healthcare averaged \$87K
- Cities/Municipalities averaged \$77K

2020 is the year of Ransomware



Organization size impacts remediation cost

Unsurprisingly, the survey has confirmed that the cost for remediating a ransomware attack is higher for larger organizations.

Average cost to remediate a ransomware attack



2020 is the year of Ransomware



Paying the ransom doubles the cost

One of the most interesting findings from the survey is that paying the ransom almost doubles the overall remediation cost versus not paying or getting the data back via backups or other means. Not only does not paying the ransom generally make you feel better because you haven't given money to criminals, the good news is that it also saves you money in the long run.

Average cost to remediate a ransomware attack

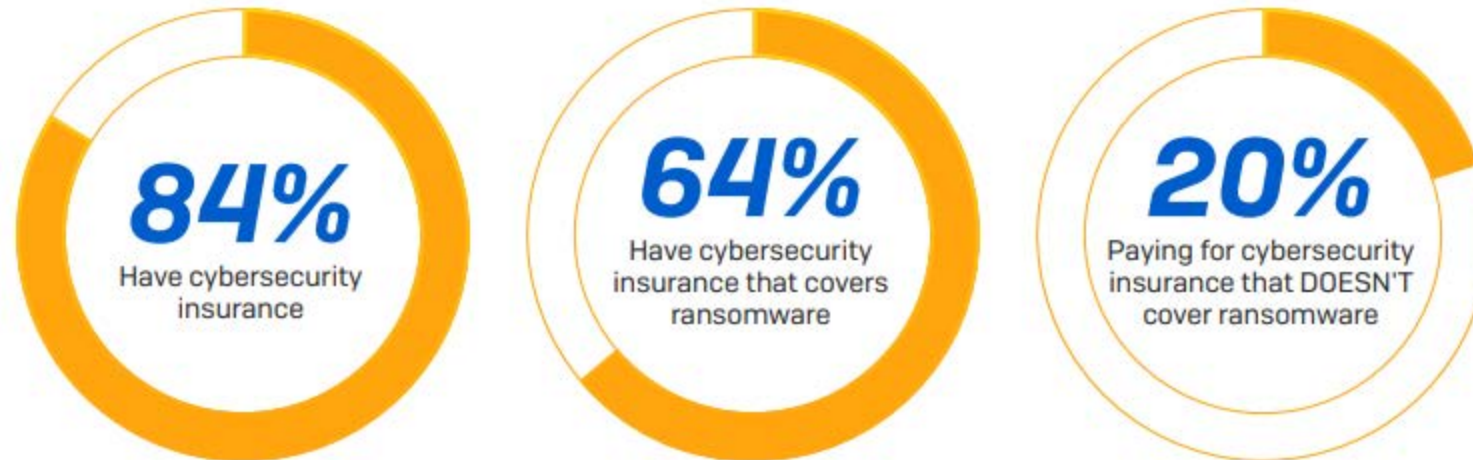


2020 is the year of Ransomware



One in five have holes in their cybersecurity insurance

Cybersecurity insurance is now the norm, with 84% of organizations reporting that they have it. However, only 64% have cybersecurity insurance that covers ransomware. This means up to one in five organizations [20%] are paying for cybersecurity insurance that doesn't cover ransomware.



Does your organization have cybersecurity insurance that covers it if it is hit by ransomware? Base: 5,000 respondents.



2020 is the year of Ransomware



Cybersecurity insurance and ransom payments

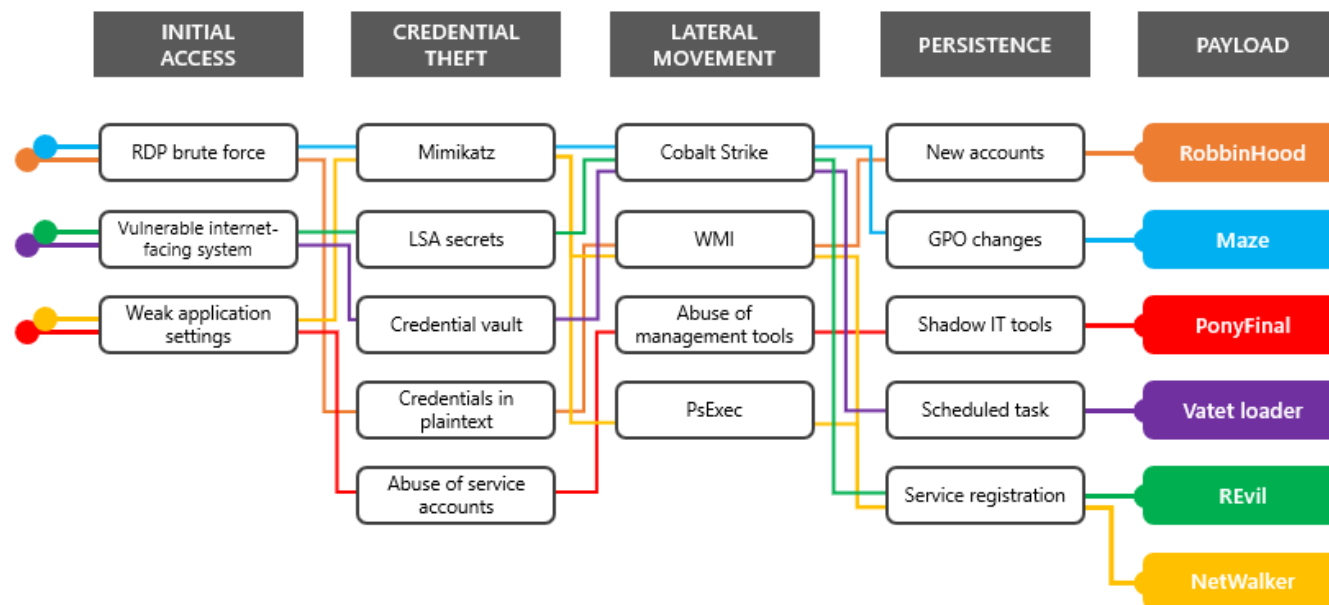
Let's now look at the role of cybersecurity in paying the ransom. As we've seen, 73% of ransomware attacks result in the data being encrypted. Of those organizations whose data was encrypted, 26% said they paid the ransom to get the data back.



How does a Ransomware Attack happen?

A Motley Crew of Ransomware Payloads

While individual campaigns and ransomware families exhibited distinct attributes as described in the sections below, these **human-operated ransomware campaigns** tended to be variations on a common attack pattern. They unfolded in similar ways and employed generally the same attack techniques. Ultimately, the specific ransomware payload at the end of each attack chain was almost solely a stylistic choice made by the attackers.



How does Ransomware happen / What Happens when it does?



Three quarters of ransomware attacks result in the data being encrypted

Traditionally, there are three main elements to a successful ransomware attack: encrypt the data, get payment, decrypt the data. In almost three quarters of ransomware attacks [73%], the cybercriminals succeeded in encrypting the data.

It is, however, encouraging is that in just under a quarter of cases [24%] the attack was stopped before the data could be encrypted. It seems that anti-ransomware technology is having an impact on the success rate of ransomware attacks.



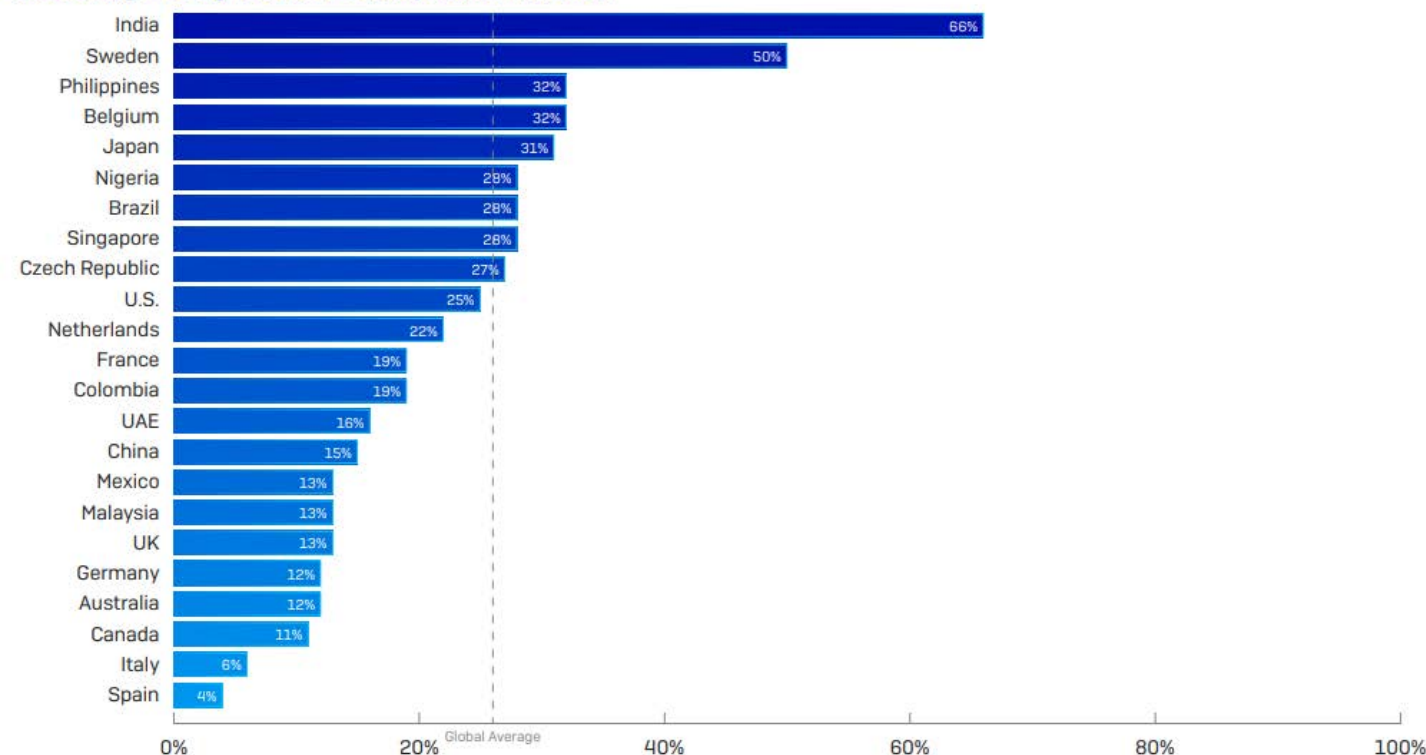
How does Ransomware happen / What Happens when it does?

26% of ransomware victims got their data back by paying the ransom

26% of those organizations whose data was encrypted got it back by paying the ransom. A further 1% of organizations whose data was encrypted paid the ransom but didn't get their data back – so overall, 95% of organizations that paid the ransom had their data restored (473 of the 496 organizations that paid the ransom).

When it comes to paying the ransom, we see some noticeable regional variations. In India two out of three [66%] paid the ransom to get the data back, while 29% used backups. Conversely, in Spain just 4% paid the ransom while 72% restored the data from backups.

Percentage of organizations that paid the ransom



How does Ransomware happen / What Happens when it does?



94% of organizations get their data back

While 73% of ransomware attacks succeed in encrypting data, the good news is that 94% of organizations affected managed to get their data back.

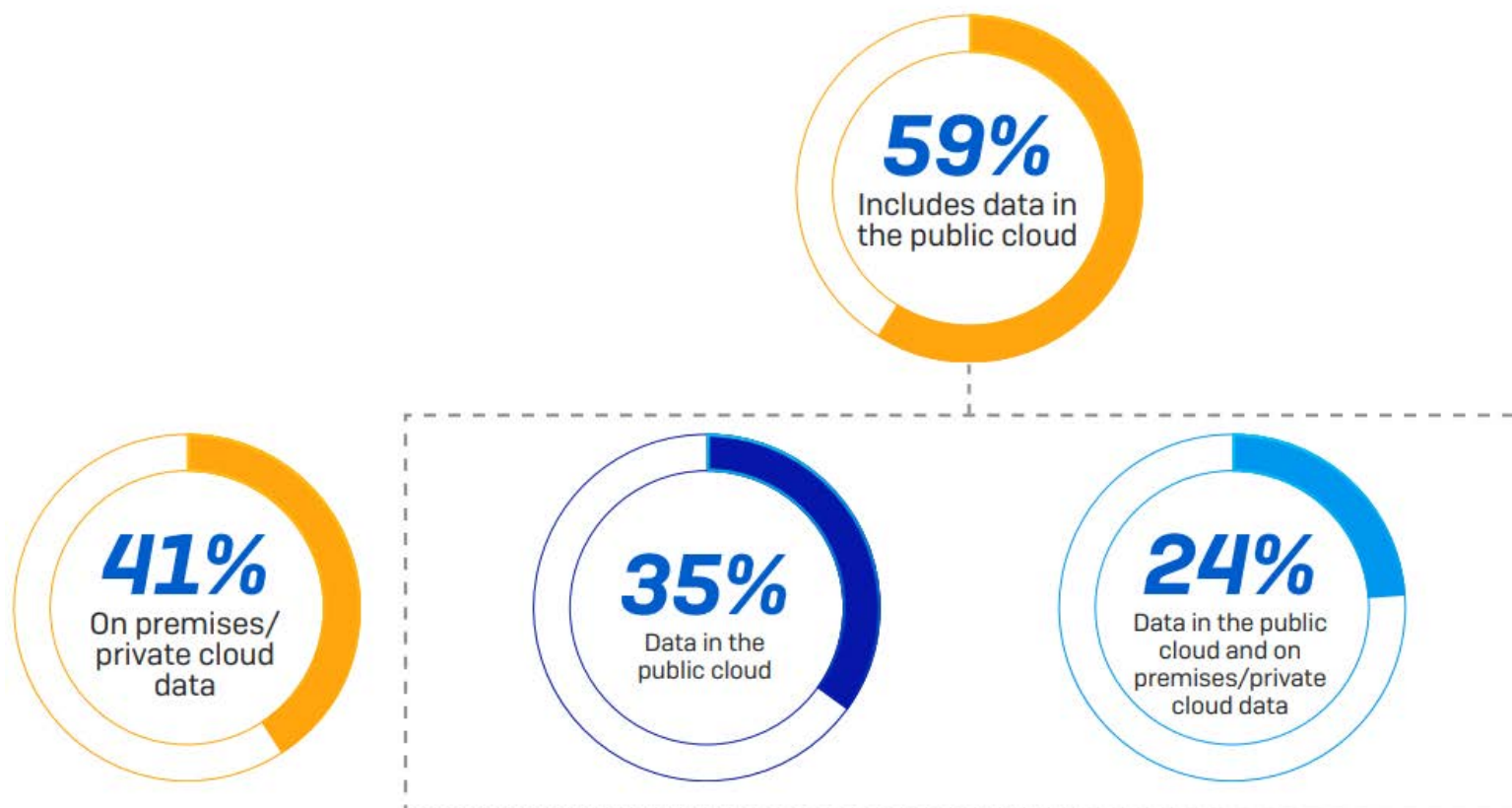
As we've seen, 26% got their data back by paying the ransom. However, more than double that (56%) restored their data using backups. The remaining 12% said that they got their data back through other means.



How does Ransomware happen / What Happens when it does?

Data in the public cloud is a mainstream target

We asked the 73% of respondents that said their data had been encrypted in the most recent ransomware attack what data was encrypted. 41% said just on-premises data and/or data in the private cloud, while 35% said just data in the public cloud. 24% said a combination of the two. Adding this up, nearly six in 10 successful attacks (59%) include data in the public cloud.



How can businesses Prevent Ransomware and/or Recover from Ransomware?

Managed Security Services

ONEteam MDR/MSOC *plus*

- ◆ Managed Detect and Response (MDR)
 - 24 x 7 Eyes on Glass
 - Managed SIEM
- ◆ Cyber Incident Response (CIR) / Forensics
- ◆ Vulnerability Management
- ◆ Managed Risk Services
- ◆ Custom Reporting
- ◆ User Behavior Analysis (UBA)



ONEteam MDR/MSOC *platinum*

ONEteam MDR/MSOC *premier*

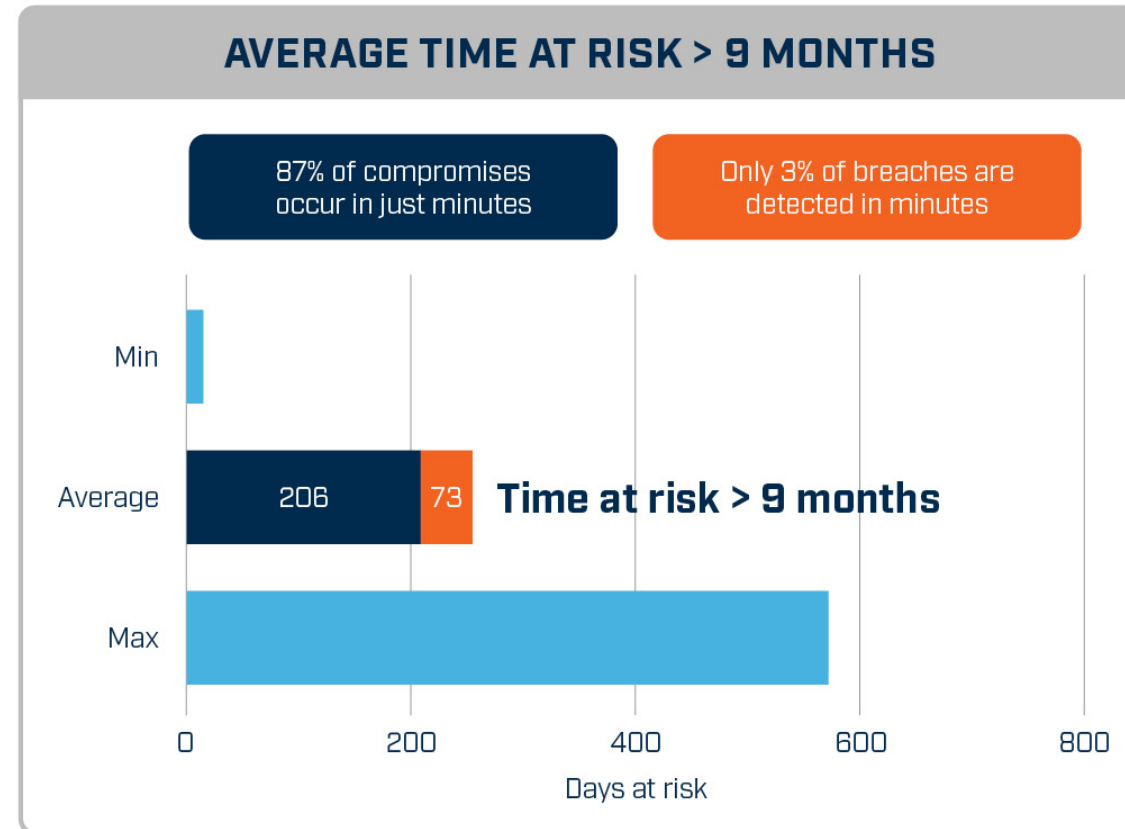
- ◆ All of *plus Service*
- ◆ Attack Simulation
 - Advanced Threat Intelligence & Hunting
 - Risk-Based Vulnerability Management (RBMV)
 - MITRE ATT&CK Heat Map
 - Managed Simulations
 - Remediation Prioritization

- ◆ All of *premier Service*, customized to contain one or more of the following:
- ◆ Managed Security Awareness / Phishing
- ◆ Managed Third Party Risk
- ◆ SOAR Solutions (automated remediation)
- ◆ Other Solutions as required

Why should MDR/MSOC matter to you ?

On average, it takes businesses 206 days to detect infections, and a further 73 days to resolve them

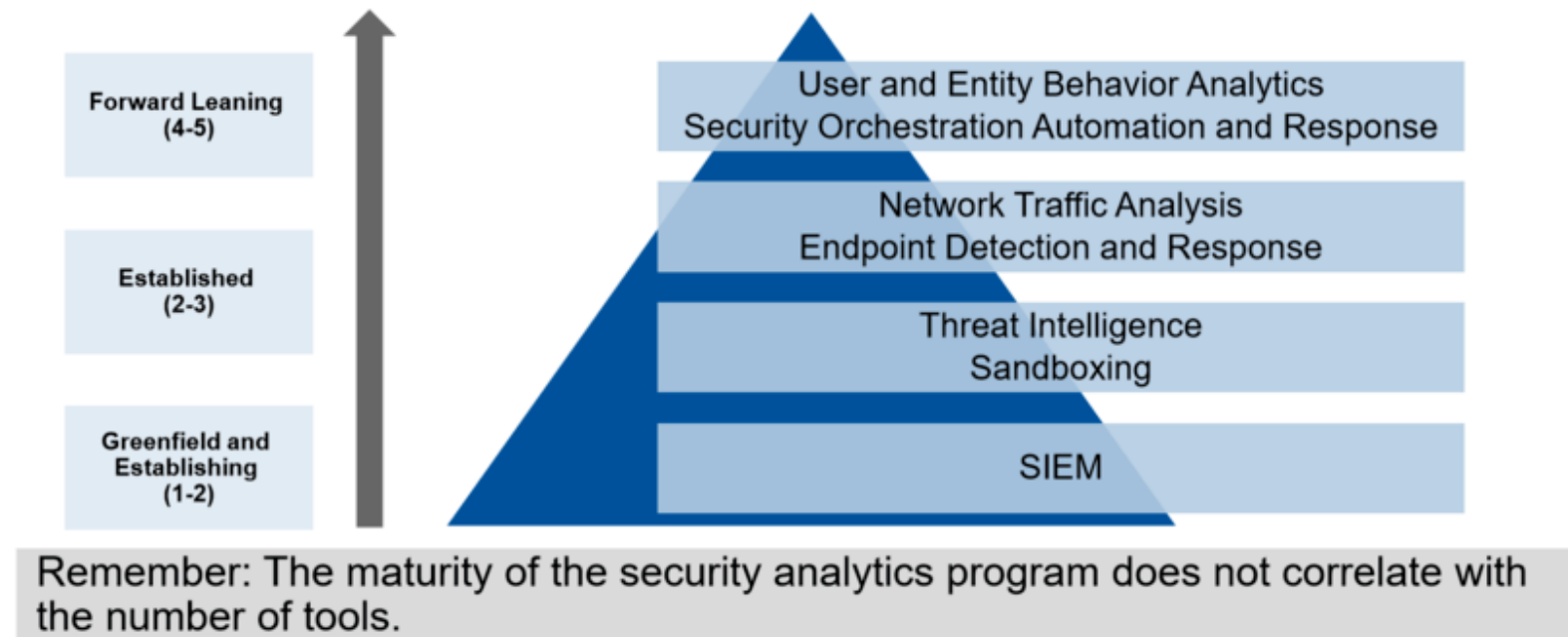
Understanding Time at Risk



■ Infection > Detection ■ Detection > Response ■ Time at Risk

*Ponemon Institute: 2019 Cost of Data Breach Study.

Modern SOC Analytics Tooling and Stage of Maturity

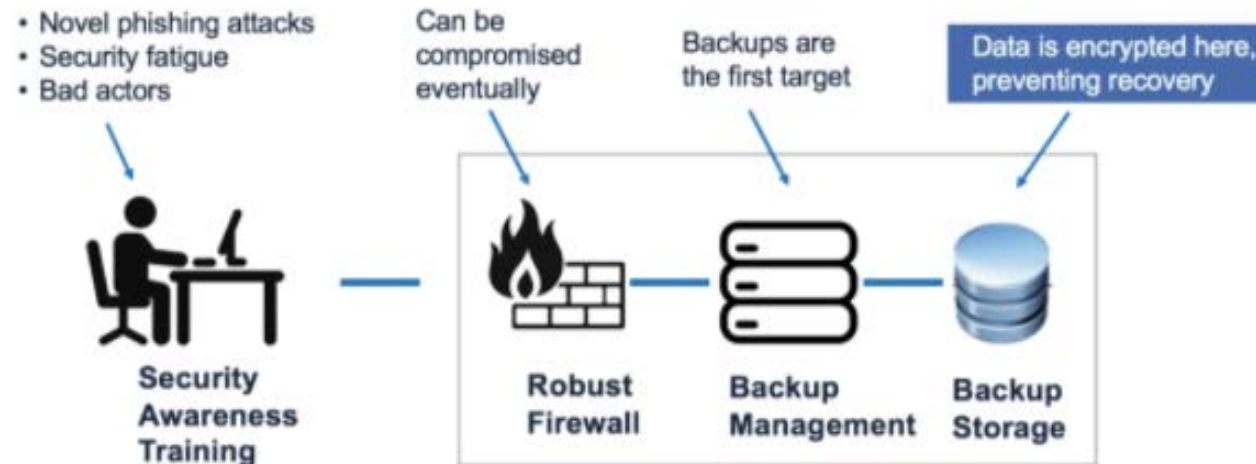


10 © 2018 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner

Architect a DR strategy using Backups

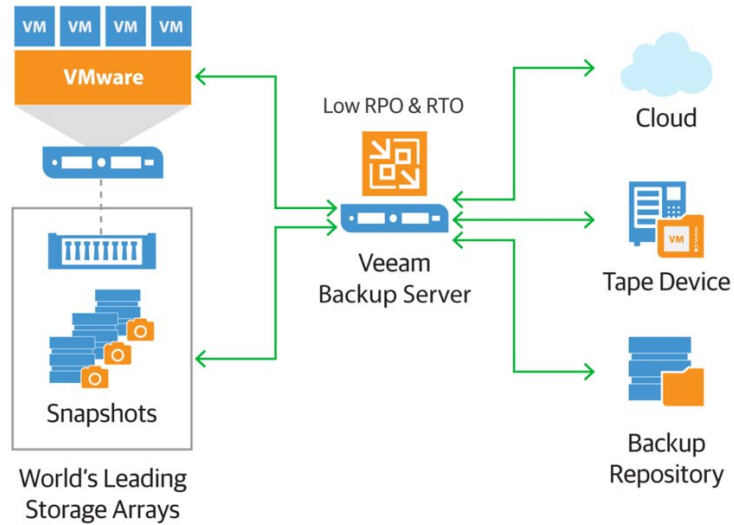
Why Traditional Ransomware Protection Fails



Ransomware protection fails when novel malware approaches circumvent even the best security training and firewall technologies

Source: VEEAM, Cloudian

Architect a DR strategy using Backups

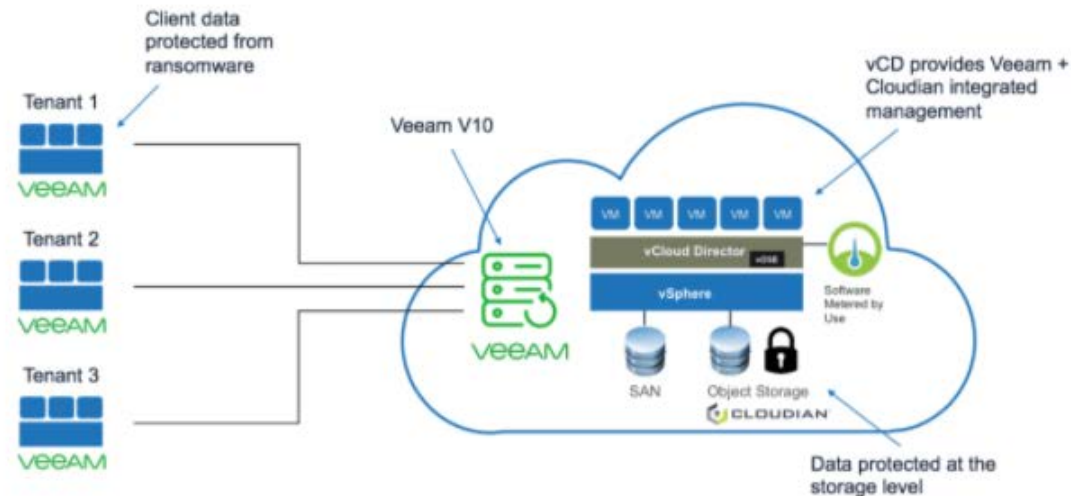


3 – 2 – 1 Backup Architecture

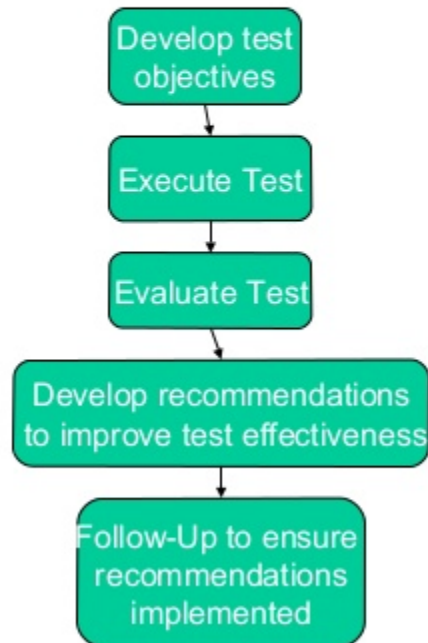
- 3 backup targets
- 2 different backup mediums
- 1 Cloud

Immutable Backups

- Lots of Options!



Testing Procedures



Tests start simple and become more challenging with progress

Include an independent 3rd party (e.g. auditor) to observe test

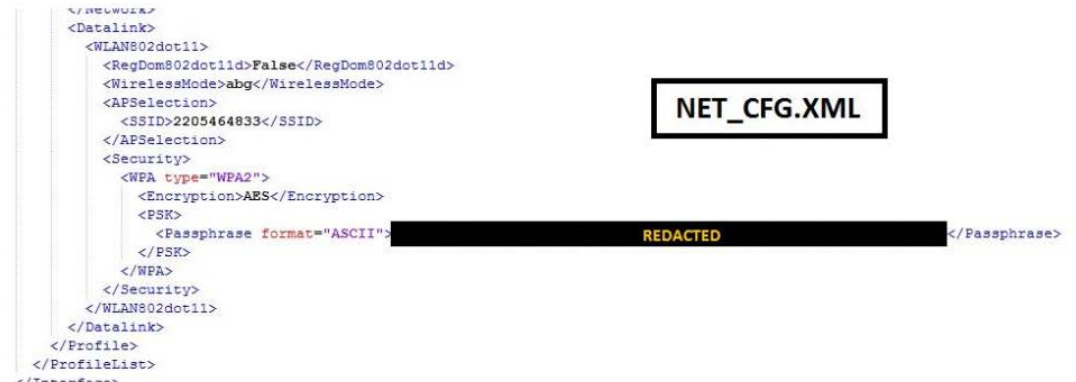
Retain documentation for audit reviews

Use Tabletop Exercises to Test your Incident Response

Introductions, Overview, and Objectives

- Presentation will include:
 - **Background** items for education to provide context,
 - **Back Story** items for event context, not known items,
 - **Breaks** opportunities to check email and reflect,
 - **Injections** as the scenario evolves,
 - **Updates** provide status for outstanding issues,
 - **IR Action** questions for direction of activities, and
 - **IR Prevention** discussion topics.
- Open discussion is encouraged.
- An **After Action Report** will highlight any Roses / Buds / Thorns identified.

Internal Network Configuration



The image shows a code editor window displaying the contents of a file named **NET_CFG.XML**. The XML code is as follows:

```
<?xml version="1.0"?>
<DataLink>
  <WLAN802dot11>
    <RegDom802dot11d>False</RegDom802dot11d>
    <WirelessMode>abg</WirelessMode>
    <APSelection>
      <SSID>2205464833</SSID>
    </APSelection>
    <Security>
      <WPA type="WPA2">
        <Encryption>AES</Encryption>
        <PSK>
          <Passphrase format="ASCII">[REDACTED]</Passphrase>
        </PSK>
      </WPA>
    </Security>
  </WLAN802dot11>
</DataLink>
</Profile>
</ProfileList>
</Tnx>
```

- The NET_CFG.XML file contains the actual wireless configuration information and password.
- That password gets you access to the internal network.

Summary – How to Prevent and/or Respond to Ransomware



Recommendations

The survey has confirmed that ransomware remains a very real threat for organizations today. It's also provided insight into how to minimize your risk of being held hostage:

1. **Start with the assumption that you will be hit.** Ransomware it doesn't discriminate: every organization is a target, regardless of size, sector, or geography. Plan your cybersecurity strategy based on the assumption that you will get hit by an attack.
2. **Invest in anti-ransomware technology to stop unauthorized encryption.** 24% of survey respondents that were hit by ransomware were able to stop the attack before the data could be encrypted.
3. **Protect data wherever it's held.** Almost six in 10 ransomware attacks that successfully encrypted data include data in the public cloud. Your strategy should include protecting data in the public cloud, private cloud, and on premises.
4. **Make regular backups and store offsite and offline.** 56% of organizations whose data was encrypted restored their data using backups last year. Using backups to restore your data considerably lowers the costs of dealing with the attack compared with paying the ransom.
5. **Ensure your cyber insurance covers ransomware.** Make sure that you're fully covered if the worst does happen.
6. **Deploy a layered defense.** Ransomware actors use a wide range of techniques to get around your defenses; when one is blocked, they move on to the next one until they find the chink in your armor. You need to defend against all vectors of attack.

Use Security Awareness Training and Phishing Tests to educate users

Use MDR/MSOC to catch intruders before Ransomware happens

Use the 3-2-1 rule for architecting backups

Use Attack Simulation to Test Controls

Key Takeaways

- ◆ *Assume you will be hit with Ransomware (Not If, but When)*
- ◆ *Have multiple data backups (3-2-1) with a focus on Recovery (RTO, RPO)*
- ◆ *Deploy MDR/MSOC for early detection and immediate action*
- ◆ *Have a detailed, up to date Incident Response Plan*
- ◆ *Be Prepared – Practice with Tabletop Exercises and DR Test Plans at least one per year, preferable quarterly*
- ◆ *Make sure you have cyber insurance that covers Ransomware!*

Q & A



ONETeam

For more information:

800 Superior Ave E, Ste 1050
Cleveland, OH 44114

Phone: 216.255.3040
Email: sales@asmgi.com

www.asmgi.com