RANSOMWARE:

These 4 Best Practices Could Save you $4M

ōrdr

Table of Contents

Introduction 3

High Profile Attacks In 2021 5

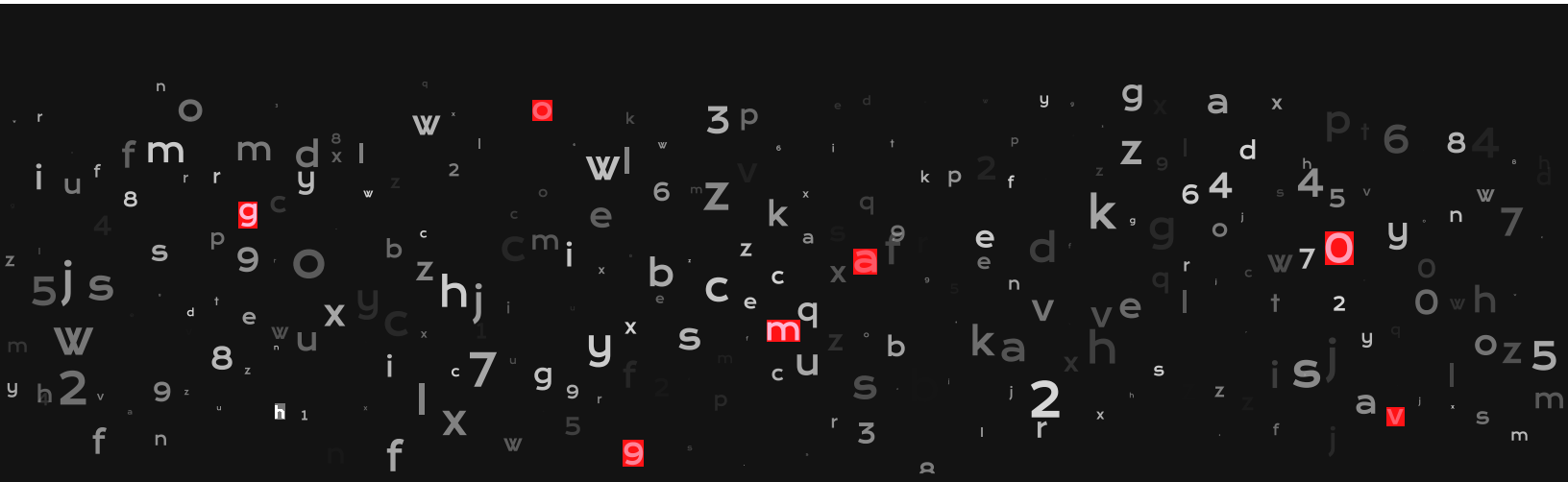
Challenges 6

Criminal Tactics 6

Ransomware Best Practices 8

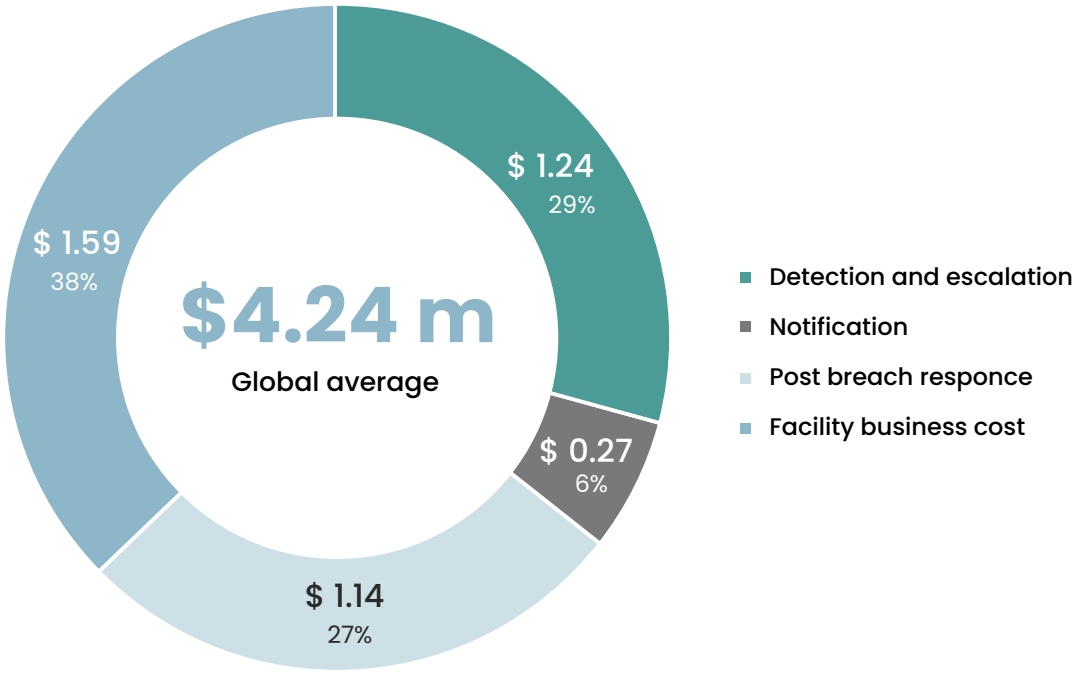
Conclusion and Next Steps 11

About Ordr 12



Introduction

Criminals are becoming more sophisticated and aggressive by the day, and security teams are increasingly under-resourced, dealing with a barrage of risks and an all-out siege on their digital assets. One of the most popular tactics has been ransomware. So far in 2021, ransomware attacks against businesses occur every 11 seconds, which accounts for over 4,000 attacks every day. The global cost will exceed $20 billion by the end of the year, with thousands of severely impacted organizations.



Source: IBM's Cost of a Data Breach Study

According to IBM's Cost of a Data Breach Study, the average total cost of a data breach is $4.24 million globally and $8.64 million in the United States. This is a 10% increase from the previous year. Ransomware attacks cost an average of $4.62 million, more expensive than the average data breach ($4.24 million). According to IBM, these costs included escalation, notification, lost business and response costs, but did not include the cost of the ransom. Malicious attacks that destroyed data in destructive wiper-style attacks cost an average of $4.69 million. The percentage of companies where ransomware was a factor in the breach was 7.8%. This is a heavy price to pay for not replacing legacy technology and an outdated approach.

The attacker's focus is shifting to leveraging vulnerabilities to infiltrate organizations' infrastructure. In IBM's 2021 X-Force Threat Intelligence Index, vulnerabilities (35%) surpassed phishing (31%) as the most common attack vector for the first time in years. The 2021 cyberattacks on the Colonial Pipeline and SolarWinds have placed a greater spotlight on the issue as companies rapidly brace to protect their digital infrastructure.

21 days

Average downtime due to ransomware attacks [2] (Coveware)

287 days

Average days it takes a businnes to fully recover from an attack [3] (Emsisoft)

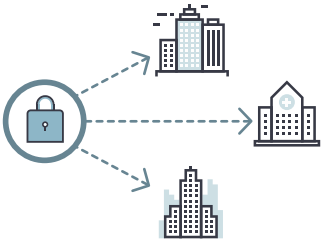
$350 million

Victims paid in ransom in 2020 - a 311% increase over the prior year [4] (Chainalysis)

$312,493

The average payment in 2020 - a 171% increase compared to 2019 [5] (Palo Alto Networks)

In 2020, nearly **2,400** U.S. - based governments, healthcare facilities, and schools were victims of ransomware

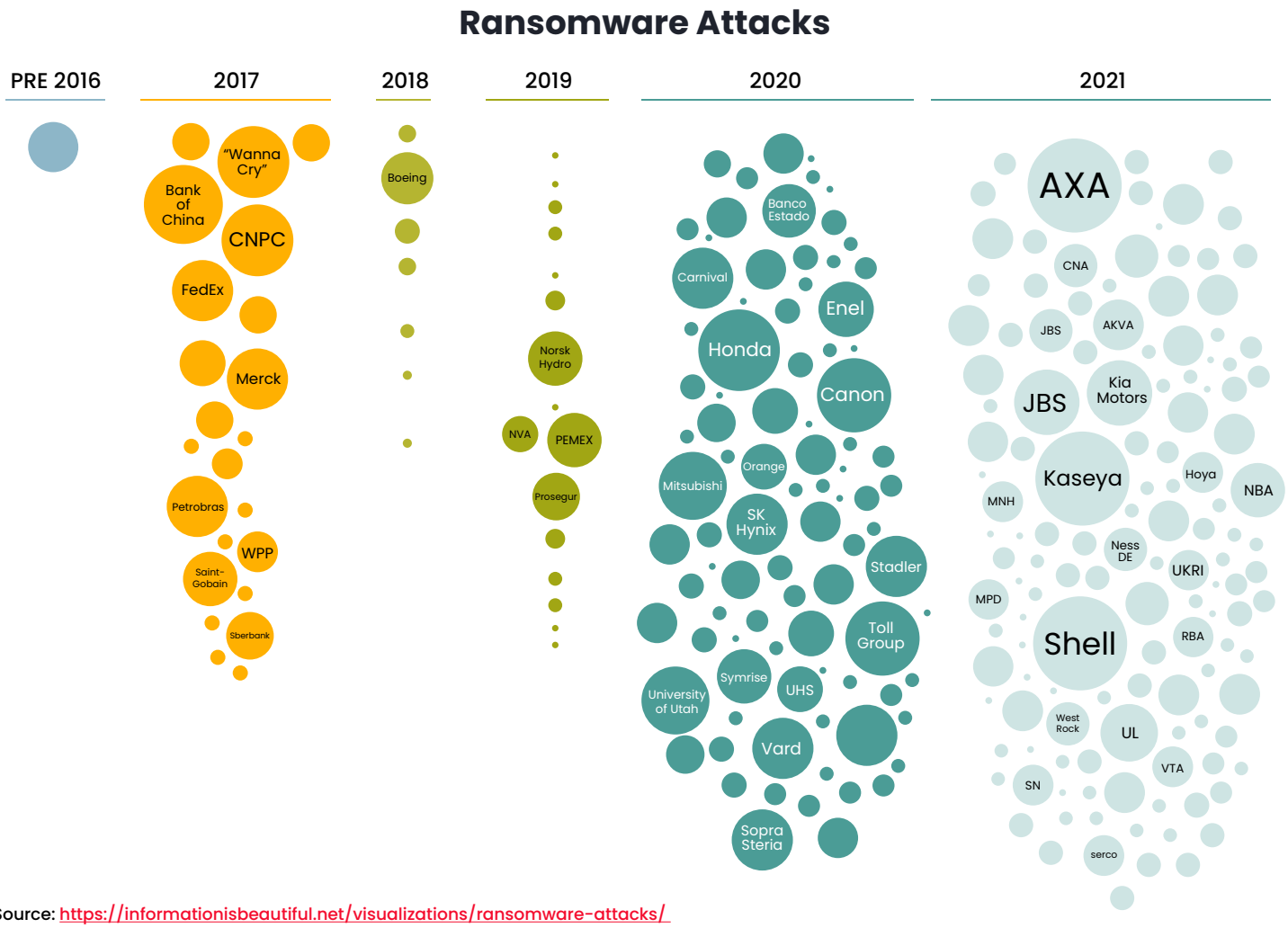


Source: Combating Ransomware - A Comprehensive Framework for Action:
Key Recommendations from the Ransomware Task Force; a 81-page report detailing a framework to combat ransomware.

On average, it takes organizations 287 days to identify and contain a breach. According to a recent SANS Incident Response (IR) Survey, 14% of firms indicate that the time between compromise and detection is between 30 to 180 days. Of those that detected an intrusion, nearly 10% said it took up to 90 days to contain. Over 42% state it takes months to over a year to resolve a threat. This delay is unacceptable given the current velocity that threat actors move inside an organization's environment once they are able to infiltrate.

High Profile Attacks In 2021

2021 has been a catastrophic year for ransomware attacks that have made it across the front page of every newspaper in every country across the world and there is no sign of it slowing down.



Source: https://informationisbeautiful.net/visualizations/ransomware-attacks/

Key Cyberattacks to Note:

- **Colonial Pipeline** - Disrupted gas supplies along the East Coast of the United States causing chaos and panic for weeks in April. DarkSide gang was behind the attack and was paid $4.4m in bitcoin which was inevitably recovered by the FBI.
- **Brenntag** - In May, DarkSide targeted the chemical distribution company after stealing 150 GB of data. A demand of $4.4m was paid and was not recovered.
- **Acer** - Also in May, Acer was attacked by REvil, the same group responsible for the attack on London Foreign Exchange firm Travelex. The group exploited a vulnerability in a Microsoft Exchange server and was able to access sensitive financial data.
- **JBS** - REvil group had a busy month but also had time to attack JBS, one of the largest meat processing companies in the world. Panic buying ensued and caused another emotional ripple effect around the globe as consumers feared a major food shortage. A massive payment of $11 million was paid.
- **Other notable high-profile attacks:** Quanta, National Basketball Association, AXA, CNA, CD Projekt Red, KIA Motors.

Challenges

To make matters worse, these figures only scratch the surface of a much larger issue. The United States is one of the only countries that have reliable and up-to-date reporting on official data breach disclosures. According to research conducted by HackNotice, who analyzed over 65,000 data breach reports from 2018 to 2020 and cross-referencing them to cybercriminal reports and unofficial channels, found that only 13% of organizations are actually reporting.

This is down from 25% last year and roughly 35% the year before. This highlights that as large as these figures may seem in terms of volume it is potentially over 7x worse than it seems on paper.

What is driving this change is the fact that cybercriminals are moving through their own digital transformation. Threat actors have built a robust underground economy that rivals the global one. It has matured to the point where less experienced or even oversubscribed criminals can leverage managed services, such as Access-as-a-Service and Ransomware-as-a-Service (RaaS), that rival industry-leading providers in terms of professional service offerings and 24x7x365 support.

Criminal Tactics

DDoS (Distributed Denial of Service)

In a DDoS attack, the threat actor targets an organization's website and/or internet facing digital assets with a flood of concentrated web traffic over an extended period of time. The goal is to overwhelm the web server to the point that it's unable to respond to requests from legitimate visitors. Several ransomware gangs are now using this joint DDoS extortion and ransomware technique to more aggressively force victims to contact them and begin negotiating. This also adds significant complexity beyond just restoring from a best-known backup.

In addition, DDoS is being used as a distraction. In situations where threat actors are now using this method to confuse and overwhelm their victims while they implement other attacks while resources are focused elsewhere.

The mere fear of a DDoS attack is also being used as a scare tactic. Phishing emails can contain malicious links that entice the victim to click on in order to prevent or help their organization in 'preventing' a DDoS attack.

It is not unusual for DDoS attacks on organizations to be followed by an increase in phishing mail to customers and end users. Criminals often attempt to use the agitation around digital attacks to make people feel vulnerable, and to then extract sensitive information like user credentials and personal identifiable information (PII). This allows criminals to infiltrate, move laterally, and further persist in an organization's environment.

Lateral Movement

In October of 2020, UVM Medical Center incurred costs of at least $50 million after an employee downloaded malware on their corporate laptop after accessing their personal email on vacation. When the employee reconnected to the corporate network upon their return, the threat actors were able to use the malware to launch the attack across the entire network.

Insider Threat

In March 2021, Egor Igorevich Kriuchkov was convicted of offering a Tesla employee $1 million USD to place ransomware in the computer network of one of the company's factories. His intent was to steal company secrets for the intent of obtaining a sizable payment. The FBI was able to stop the attack, with help from the victim, before it could take place. This is a sobering reminder that criminals will go to any lengths to achieve financial gain.

Extortion

Doxware (also known as Leakware or Extortionware) is ransomware that extorts victims by threatening to release sensitive information if a ransom is not paid. According to BlackCloak, a company that provides cyber protection services for corporate executives and high-profile individuals, "The combination of spear phishing (personally crafted and targeted messages) with ransomware makes executives and other high-profile individuals a growing target base. The attackers know exactly who they're after and use personal information to make their messages appear plausible. Most ransomware hits small businesses and personal systems, which are often easy targets and willing to pay, but the overall trend is toward hand-picked targets that can pay large amounts."

Criminals will often target the victim's family in order to coerce them into payment. By compromising IoT devices, internet connected video gaming systems, and personal laptops inside the home they can gain access to sensitive information in order to provide necessary leverage to extort their true target.

IoT

There are 28 billion IoT devices in the world and counting. They are literally everywhere. Many of them do not have a logical interface and therefore do not have a way to protect themselves. In particular, with inferior off-brand products, users do not have the ability to update their software or have the ability to implement a password let alone one that allows for multi-factor authentication. For those that do, many users forget to change the default password.

Introducing this new attack surface inside of a corporate environment could have dire consequences. Imagine what would happen if a patient, visitor or employee brought an IoT device into a hospital, factory or power plant. It wouldn't take long for a threat actor to use an open-source software like Shodan to discover, compromise and infiltrate the network.

The Multi-Punch Combo for the TKO

On July 27th, the Senate Judiciary Committee held a hearing, "America Under Cyber Siege: Preventing and Responding to Ransomware Attacks" that featured testimony from senior officials from DoJ, FBI, CISA, and the US Secret Service (USSS).

In his testimony, USSS Assistant Director, Office of Investigations Jeremy Sheridan wrote, "Year-over-year, the U.S. Secret Service has observed a marked uptick in the frequency, sophistication, and destructiveness of ransomware attacks against the American people." He also discussed the trend of "double" and "triple" extortion where "ransomware actors also began experimenting with adding additional extortion demands, often referred to as 'double extortion.' Criminals now sometimes demand two separate ransom payments, the first to unlock a frozen computer network, and then a second to prevent the public disclosure of stolen information. Some are even extending this practice to 'triple-extortion,' adding denial-of-service attacks to further pressure victims of these extortion schemes."

Ransomware Best Practices

Back in 2019, after conducting hundreds of interviews with corporations that had experienced a data breach, Brad LaPorte came to one conclusion, over 90% of them were all preventable. This research was documented in Defend Against and Respond to Ransomware Attacks.

> *"Gartner analysis of clients' ransomware preparedness shows that over 90% of ransomware attacks are preventable. These attacks pose a threat to business data and productivity, but by following basic security fundamentals security and risk management leaders can mitigate risk against them."*
>
> **- Brad LaPorte, Gartner Veteran & Industry Expert on Ransomware Prevention & Response**

In the past two years, LaPorte's guidance as industry expert and Ordr advisor remains relatively the same. The best practices are to focus on the basics.

4 things you can do to mitigate the impact of a ransomware attack:

1. Focus On the Basics and Drill Often

By focusing on basic cybersecurity hygiene organizations can greatly reduce their risk against ransomware attacks.

- Fully understand your attack profile. Conduct security assessments and tests to determine the attack surface and current state of security resilience and preparedness in terms of tools, processes and skills to defend against attacks.
- Implement MFA on everything that will allow it.
- Embrace micro-segmentation architecture by dividing the entire digital environment into smaller parts to mitigate the impact if one part is compromised.
- Harden your assets in priority order in accordance with your business continuity and disaster recovery plans.
- Encrypt all data, whether stored or transmitted. In the event of a data breach, critical files should only result in unusable data.
- Conduct regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices.
- Regularly patch and update software and OSs to the latest available versions.
- Ensure devices are properly configured and that security features are enabled. Implement high enforcement restrictions for all remote desktop services (e.g. Remote Desktop Protocol or RDP).

*Note – See CISA's official guidance on reducing your exposure to a ransomware attack for more information

2. Have a Plan (Embrace Ransomware Response Governance)

Establish processes and compliance procedures that involve key decision-makers and stakeholders in the organization. This needs to be completed well in advance before preparing for the technical response to a ransomware attack. Ransomware can escalate from an issue to a crisis in no time, costing an organization significant financial loss and creating a damaged reputation.

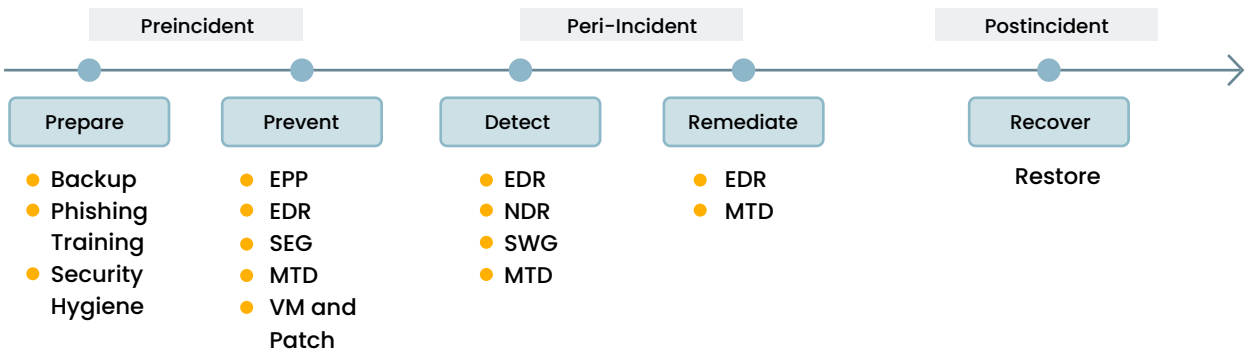
Key people such as the CEO, CISO, CIO, board of directors and other important stakeholders must be involved in the preparation. For each part of ownership establish a well-defined RACI model along all five phases of Gartner's Ransomware Defense Model.

RACI Chart

Responsible — Person who is responsible for executing or doing the activity
Accountable — Person who owns, approves, and is the final decision-maker for the activity
Consulted — Person who can provide further information or feedback for performing the activity
Informed — Person who only needs to be informed about the activity's progress or status

	Overall coordination	Media messaging	Internal communications	Customer communications	Technical assistance	Regulatory body liason	Maintain records	Post-incident report
CIO/CISO	A	I	AR		I	I		
Incident management team coordinator	R	C	C		A	I	AR	AR
Security operations lead	I				AR	I	R	C I
Business manager	I	C	C		C			C I
Media and public relations manager		AR	I	C				I
Managed service provider (MSP)	I				R		C I	C

The Five Phases of Ransomware Defense



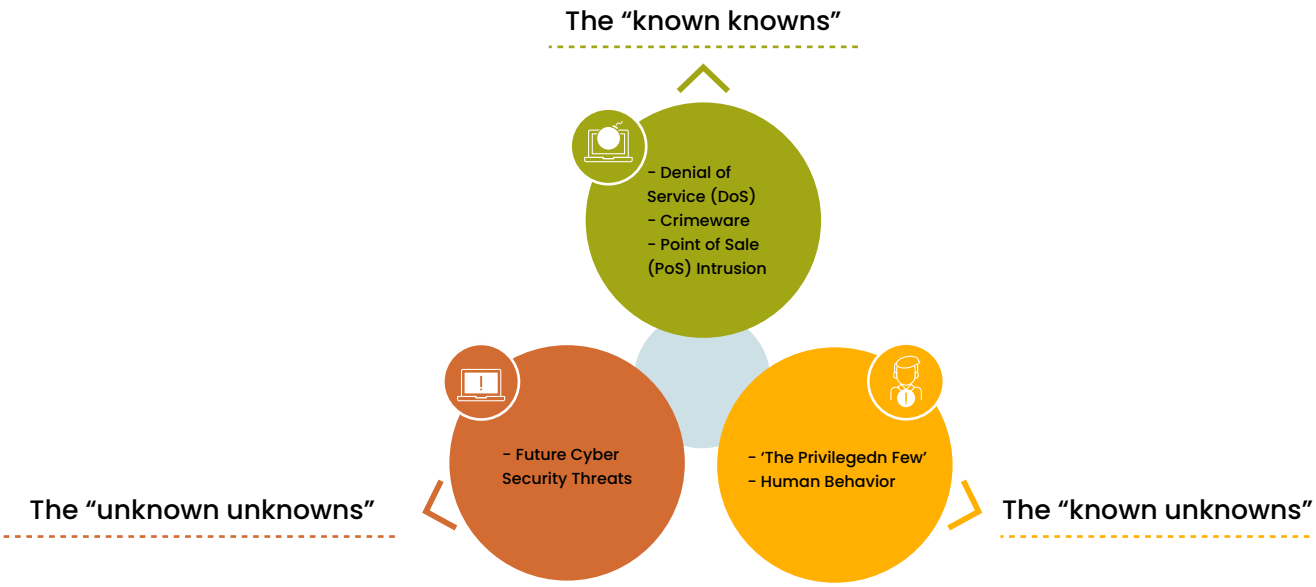
Source: https://www.gartner.com/en/documents/3987751/designing-and-implementing-a-ransomware-defense-architec

3. Continuously Improve (Maintain Continuous Operational Readiness)

> *"...there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns — the ones we don't know we don't know."*
>
> **– Donald Rumsfeld**

Known unknowns are risks related to things that you know, and you can plan for, such as the risk of using new technology for a purpose. The purpose might change, or the technology may not perform as intended. The unknown unknown is something that you don't even know because it never existed before, such as the COVID-19 pandemic that changed the world forever.

This core concept applies to cybersecurity just as it does to any global threat. Organizations need to start their readiness operations today and continually improve. Operational readiness aims to improve organizational security posture while simultaneously reducing risk exposure. The intent is to address weak points and blind spots in the organization's virtual armor before it becomes a crisis.



A note on data recovery backups: Always back up not only all of your critical data but also every nonstandard application and its supporting IT infrastructure. This a very important step but should never be considered a bulletproof approach however. Backup systems protect your most valuable asset, the data, but an experienced cybercriminal who has access to the administrative account of the backup servers can prevent backups from being used to recover data. Attacks often have a delayed time element associated with the attack. The purpose is to ensure that the golden copy is affected (typically more than 90 days), or that long-term backs and even archives are also affected. Without knowing these key components of the attack, the recovery could be short-lived and bring business operations to a screeching halt and stay there for good.

4. Implement Zero Trust

Only the users that need to access specific information at specific times should have access to that data. Leaders must restrict permissions and deny unauthorized access to devices. Remove local administrator rights from users and block application installation by standard users, replacing this with a centrally managed software distribution facility.

CISOs and security leaders must deploy multi-factor authentication wherever possible, prioritizing privileged accounts. It is critical to increase authentication logging on all critical servers, network devices, directory services, and ensure logs are not modified or deleted. Security teams must prioritize monitoring of any unexpected activity and ensure they proactively look for unusual logins and/or failed authentication attempts.

Conclusion and Next Steps

What can we expect in the near future?

The Colonial Pipeline attack hearings were a wake-up call for enterprise CEO across all industries and geographies. Recent events now have the attention to the highest levels of government. This has cascaded down and law enforcement capabilities have greatly increased with Cyber Insurance Underwriting running in the opposite direction.

The US is not alone in their struggle against threat actors that wish to do them harm. This is highlighted in recent events in Germany, Canada, Australia, United Kingdom as well as other many other nations and industries.

Ransomware as an industry is here to stay. While law enforcement tracks ransomware groups, and legislation is developed to bring ransomware threat actors to justice, we must rally as an industry to share threat intelligence and do what we can to protect our business and our critical infrastructure. This is the new cyberwar.

About Ordr

Ordr Systems Control Engine (SCE) delivers visibility and security for every connected device. Our solution is agentless and SaaS-based. There is no impact to any device that we discover and secure. Within a few hours of deployment, our platform discovers every connected device, profiles behavior and risks, and automates action.

Ordr is here to help you prepare for a ransomware attack and to quickly mitigate risks if you're under attack. Here's how organizations are using the Ordr Systems Control Engine today for agentless visibility, threat detection and response:

1. Identify and understand ransomware risks for every device

Ordr uses DPI and AI, along with enrichment from a variety of different security and threat intelligence sources to calculate the risk and security posture of every device. Device context including attributes like O/S of the device, hotfixes deployed, installed software deployed, and the behavioral patterns of the device provides a unique view of the risks of a device. Ordr uses industry-leading threat intelligence to detect close to 25 critical event types to identify vulnerable devices in the network, and offers an actionable risk score.

2. Track East-West lateral movement with Ordr Threat Detection Engine

Ordr sensors deployed across the network support the full stack L7 threat detection capabilities. Most organizations focus on north-south threat detection, but east-west traffic analysis is critical to lateral movement and is a major blind spot for enterprises as this analysis is outside the realm of perimeter firewall. Ordr detects exploits, recon and privilege escalation, tools used in attacks (Eternal Blue and Cobalt Strike) and more.

3. Monitor communications to ransomware domains

Ordr monitors and tracks C2 communications to malicious entities associated with ransomware campaigns such as DarkSide, Ryuk, Conti and more. Ordr SCE also supports capabilities to analyze traffic retrospectively for these communications.

4. Customized security event monitoring

Users can monitor for specific IoCs associated with a threat actor campaign, This will create a new entry in the Ordr Group Traffic Analysis constellation view. Users will have an option to drill down the communication patterns of each device associated with the event.

5. Automated response

The most critical aspect of a ransomware attack is determining what device is compromised, where it is located, and whether mitigation is possible. Ordr's granular insights about devices including make, model, serial number, location in the network, along with complete details about every device communications patterns are critical to determine whether to and how to take action during an attack. For example, a non-critical video surveillance camera can be immediately removed from the network, but a critical manufacturing device may need to be isolated while keeping the device in operations. Ordr automates the creation of NGFW policies, ACL blocks, quarantine VLAN assignment, port shutdown, or session termination with one click of a button-- enforced on existing switches, wireless controllers, and firewalls, or via NAC platforms.

We've helped hundreds of organizations on their cybersecurity journey, and we are eager to partner with you on yours. Ordr is backed by top investors including Battery Ventures, Wing, and TenEleven Ventures. Reach out to us at www.ordr.net today and schedule your Ransom Aware Assessment.