lightstream

THE MID-MARKET GUIDE TO SURVIVING A RANSOMWARE ATTACK

A blueprint of actionable steps focused on preparedness so you can get back to business faster.

LIGHTSTREAM
208 N 2100 West, Suite 200
Salt Lake City, UT 84116
Phone: 877-95-LIGHT

Follow us on

Let us tell you more about the amazing things we do.

RANSOMWARE TARGETS ORGANIZATIONS OF ALL SIZES

Willie Sutton has often been quoted as saying when asked why he robbed banks —

"I rob banks because that's where the money is."

While Willie has denied ever uttering the words, they ring true for ransomware nonetheless today. Ransomware targets organizations of all sizes, maturities, and industries because to be frank — it's profitable.

Ransomware has, much like other criminal enterprises in the cyber realm, verticalized and developed an entire ecosystem designed to operate with efficiency and scale. Ransomware continues to evolve and organizations that fail to plan for an attack are setting themselves up for catastrophic failure.

Business leaders in mid-market companies have lulled themselves into a false sense of security with the belief that ransomware targets only large enterprises who can afford to pay up millions of dollars in ransom. The harsh reality is that every organization, large and small alike, have valuable data that a ransomware actor can hold for ransom. In fact, modern ransomware criminals strike with clinical precision and can cripple businesses in seconds. Your business must adapt to meet the threats posed by ransomware — as the threats evolve, so must your approach and preparedness.

Being prepared for ransomware isn't just installing the latest technology and declaring success. Effective ransomware strategy must be simple, efficient, and cost-effective utilizing modern approaches to modern problems.

The 5 P's of Preparedness	
1	PROGRAM
2	POLICY
3	PLAN
4	PEOPLE
5	PRACTICE

TECHNOLOGY + AUTOMATION

"As a breach coach who spends most of my time helping companies recover from ransomware attacks, I have found that their level of preparation is commensurate to their resilience. Those companies that have a plan for how they will respond to an attack and have a team that understands their roles and have practiced their plan will almost always be much more successful at recovering from these attacks and minimizing their risk and operational downtime."

— Shawn Tuma, Partner | Spencer Fane LLP

THE RANSOMWARE LIFECYCLE

Phishing emails, RDP exploitation, and exploitation of software vulnerabilities remain the top three initial infection vectors, and are increasing.

01 | INFECTION
Ransomware can find its way onto your corporate's assets through exploitation of open vulnerabilities, an employee who clicks a phishing link, or a mis-configured cloud asset

02 | COMMUNICATION
Ransomware beacons back to its control network, where attackers decide what havok it will wreak on your network

03 | DISCOVERY
Ransomware often has built-in mechanisms to discover specific types of sensitive information for ransom, identify backup mechanisms and other defensive measures, and maximize its impact to your business

04 | DATA EXFILTRATION AND/OR BACKUP DESTRUCTION
Ransomware components will silently corrupt or disable backups and not only encrypt your sensitive information but steal it first

05 |ENCRYPTION
Your data is silently, selectively encrypted rendering your systems, applications, and sensitive data useless without decryption

06 | RANSOM DEMAND
Ransomware criminals will typically put-up graphics or email victims making ransom demands in Bitcoin to get your data back

07 | NEGOTIATION
Some ransomware gangs will negotiate, but professional ransomware negotiators also have their fees

08 | DECRYPTION?
While it's still a gamble, paying a ransom can lead to successfully retrieving decryption keys which unlock your data; but there is no guarantee that your stolen data won't be leaked or re-encrypted

280 days
The average time it takes to identify and contain a data breach[1]

68.5%
Ransomware is on the rise, from victomizing an estimated 55% of companies globally in 2018, to over 68% by 2021[2]

1 https://www.ponemon.org/
2 https://www.statista.com/statistics/204457/businessesransomware- attack-rate/

THE 5 Ps OF PREPAREDNESS

1 Program

Your ransomware strategy and plan must be part of a larger cyber security program — developed in collaboration with your IT peers and adopted up to the board level. An effective program is often aligned with the NIST Cyber Security Framework and incorporates all 5 key aspects: identify, protect, detect, respond, and recover. Bringing together strategy, technology, effective operations, and adoption will minimize the operational and financial impact a ransomware incident can have on your organization and your ability to operate your business.

2 Policy

An effective ransomware policy will set out the approach to ransomware — such as whether your organization will attempt to make a payment, and if and how you'll maintain the financial capability (such as Bitcoin wallet) in a separate legal entity, for example. A written policy that is approved by leadership and the board will structure the approach to ransomware in legal and strategic framing — so that a plan can be developed within those boundaries.

3 Plan

The ransomware plan must be three things — concise, comprehensive, and simple. Your plan must include the appropriate leadership from the enterprise and your outside support such as a breach coach, empower those people with decision-making capabilities to take action, and be as simple as possible so that in an emergency the rules and steps are clear and simple to execute under severe pressure.

4 People

An enterprise ransomware strategy must include the appropriate people. From your organization there must be strategic — such as executives and legal representation, and tactical — such as technical security staff representation. You must also include outside parties such as local and federal law enforcement, specialized lawyers, negotiators, insurance firms, and forensics organizations. These people's roles must be clearly defined, their contact information provided, and they must all be aware of their role in the plan.

5 Practice

A ransomware strategy that is not extensively tested and practices is a liability. Your organization must practice and test its ability to organize, execute your plan, and improve its response capabilities. A combination of table-top exercises, backup restore exercises, and catastrophe drills should be utilized to ensure that your organization is not only prepared in theory, but also has the muscle memory to execute under pressure when the business is on the line.

THE ROLE OF TECHNOLOGY

Enable your business to move faster and more securely by applying a zero trust security strategy to selected, outcome-focused initiatives.

Technology has a strong supporting role to play in ransomware strategy. Technology is applicable at all 5 areas of the NIST CSF — covered here for incorporation into your cyber security program, and ransomware strategy.

Identify | technology should be leveraged to operationalize the identification (data discovery) of critical and sensitive data as part of a data governance and protection program. Additionally, technology enables the rapid and automated detection and classification of unknown assets (through attack surface management), and threats to those assets.

Protect | Technology for protecting data and individual assets is well-established and available for self-management and as a service. Whether it's at the endpoint, or at the data layer – technology enables the prevention of known threats and attack patterns, raising the bar for attackers and cyber criminals if deployed and operationalized effectively.

Detect | Effective technology to detect cyber-attacks and malicious software is widely available in the marketplace. The largest obstacle to identifying attackers and present threats is effective operationalization of these technologies. Effective implementation requires round-the-clock security operations staff and processes to decrease the amount of time an attacker has after successfully establishing a foothold in your IT. A critical operational metric here, mean-time-to-detect (MttD) is something to keep focus on as you deploy tools and build processes, or partner with external Security Operations Center (SOC) providers.

Respond | Response is perhaps one of the areas where technology can be an advantage for defenders, especially in ransomware cases. If a technology platform is well-operationalized and integrated, a ransomware detection in one part of the organization can rapidly be quarantined — containing the threat, and possibly removed automatically causing minimal disruption to the overall business operation.

Recover | Technology for backing up has been available for a long time. But as people who have been through a ransomware incident can tell you – it's not the backup that's important, it's the effectiveness of the recovery. A recovery strategy should include everything from restoring a single system or data store from backup to systematically rebuilding an entire network or cloud deployment – and technology is integral to being able to perform this type of task at scale and with confidence.

Zero Trust

Zero Trust is a fundamental shift in network, application, and systems design. Zero Trust starts with the premise that no interaction, at any level, should inherently be trusted, and therefore sets up each system or application to protect itself from every other. Starting with implementing strong multi-factor-based federated identity management and working to network and data segmentation — Zero Trust is more than a theory. Zero Trust must be implemented in technology, in policy, and rooted in strategy otherwise it will fail.

A business IT platform built with Zero Trust principles — even not fully implemented — has the ability to defend itself even if there is an attack in progress by minimizing the impact any one compromise or attack can have on IT and business operations throughout the company. Minimizing impact — mainly operational and financial — to the business is at the core of Zero Trust, and a reason why your organization should be looking to implement this strategy in your overall security, and ransomware strategy.

Curiosity to solve the complex drives us

We live in the age of constant business transformation.

The Cloud, Big Data, AI and the Internet-of-Things open limitless possibilities—and even more expectations.

And with those expectations comes unfathomable complexity. Addressing them requires amazing strategy and execution of integrated technologies—all networked to provide greater visibility, predictability and cognition.

Fortunately, we've envisioned this day coming for a while.

We've addressed enterprise complexities of on-premise, in-the-cloud, and all the networks in between. We've offered solutions that drive business transformation. And we've worked to find more ways to help you meet higher expectations.

We are Lightstream.

Our passion to serve customers and our curiosity to solve the complex drives us.

We listen to and work with you to carve a path where vision and execution intersect—enabling new capabilities, driving efficiency, and spurring innovation and growth.

Because when you work with a partner who helps you understand where you can go and how to get there, complexity can be averted and every possibility can be realized.

That's where we live—and that's where we're ready to take you.

Complexity Averted. Possibilities Realized.

We've helped many public and private organizations to establish and implement a Zero Trust approach, both before and after the adoption of remote and hybrid work schedules. For a one-on-one consultation to discuss how to ensure your cloud is secure, contact us now.