EBOOK

BISHOPFOX

The Offensive Security Guide to

RANSOMWARE READINESS

Table of Contents

Introduction

THIS EBOOK IS FOR CYBERSECURITY PRACTITIONERS WHO WANT TO UNDERSTAND:

UNDERSTAND your organization's current state of ransomware readiness.

IDENTIFY gaps in your current strategy that need to be mitigated.

PREPARE your defenses and playbooks for ransomware attacks.

MEASURE progress to continually enhance your state of ransomware readiness.

> *There's nothing particularly special about how ransomware attacks begin, only in how they end.*

In 2020, companies around the world spent more than $18B in ransoms.

And what's worse...this astronomical sum does not include the costs of downtime as teams scramble to get their operations back online, protect critical shareholder and customer relationships, and navigate a legal minefield – all during a crisis.

Many ransomware attacks can destroy business operations for companies big and small – either as a temporary costly setback, as a forever black mark against their reputation, or, more often, both. During a ransomware attack, the specific outcome may remain uncertain, but disruption is inevitable, and the threat of data destruction (and perhaps worse, sensitive data disclosure) looms large.

Most experts agree that prevention is the best approach to combatting ransomware, making ransomware readiness an essential for today's enterprises. The challenge is: technology can only take us so far. The latest ransomware exploits bypass traditional controls, use authorized credentials, and insert malicious code into legitimate processes. Despite advancements in prevention technologies such as NGAV, application control (allow-listing/deny-listing), detection and response (EDR, XDR, and SOAR) and IR frameworks like MITRE ATT&CK, ransomware attacks continue to escalate.

The inconvenient truth is that threat preparation, particularly for high-stakes threats like ransomware, requires a whole-company approach. And with any group endeavor, it's essential to have the right plan, assemble the right folks, and use the right metrics to measure and communicate your progress.

We'll provide a roadmap to get your extended team aligned on ransomware readiness, by aiming to answer the following questions.

ATTACK SURFACE AREA

Do you know how and where you're vulnerable to a ransomware attack?

THREAT DISCOVERY

Which discovery methods can you employ to determine your greatest areas of exposure?

OFFENSIVE SECURITY

When it comes to options—penetration testing, red teaming, purple teaming, or tabletop exercises— which will work best for you?

RISK REDUCTION

What can you expect to learn from these programs? How do you leverage lessons learned to enhance security on a continual basis?

OPEN-SOURCE COMMUNITY

Which open-source tools can you use to start a program on your own? How do they function, and what are their use cases?

Profiling the Ransomware Attacker

PRO-TIP

When trying to unpack how a ransomware attack happens, don't restrict your analysis to atomic artifacts like IOCs, file hashes, binaries, process trees, and other technical detritus. Remember, there are actual people behind these attacks. Increasing your knowledge of their motives and operations enhances your technical understanding and helps prepare your defenses.

TO BETTER PREPARE FOR A RANSOMWARE ATTACK, UNDERSTAND THE FOLLOWING ABOUT YOUR ADVERSARY:

MOTIVE	MODE	METHODS	MOVES
What drives them to target their victims and launch attacks?	How can their behavior be characterized? What does it tell us?	What tools do they use, and how do they use them?	Once they're in, what's next?

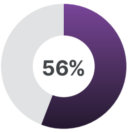
MOTIVE: PROFIT

The Attacker's Goal: If It's Valuable to You, Then It's Valuable to Them.
Back in the day, attackers targeted assets or data with intrinsic value: credit card numbers, credentials, personally identifiable information – basically any data that could be sold on black markets. One of the major innovations of ransomware groups is the monetization of the compromise itself.

If you're an architecture firm, you're not sitting on a mountain of sensitive data like a payment processor would. This simple fact used to shield specific industries from attack since they didn't own anything of value to attackers. Your typical cybercriminal doesn't care about the in-progress blueprints to a new building, after all.

But soon, attackers realized that if it has value to you, that value can be extracted. By locking up your data and selling it back to you, money could be made from almost any business.

The arrival of Bitcoin provided an easy way to transfer that value anonymously over the internet with no pesky intermediaries, and thus the market was made. In fact, in 2021, 56% of victims paid up.



MODE: OPPORTUNISTIC

The Attacker Mantra: Get the Goods and Move On.
Ransomware attackers are interested in finding the path of least resistance to a goal that will make them money. This means that they're most likely to exploit known vulnerabilities rather than spending weeks probing a custom application for something completely novel. Making sure there's no low-hanging fruit in your environment can go a long way in deterring this kind of threat.

This is in stark contrast to politically motivated attackers or hacktivism. These hackers are interested in a specific target and will evade detection on their way to get it. While any attacker prefers easy targets and will actively seek them, politically motivated adversaries are more likely to spend time and resources finding the hard way in.

METHODS: OPERATIONALIZED

Ransomware is Big Business – A Thriving and Competitive Ecosystem.
For ransomware to be profitable, the victim has to pay the ransom. This sounds obvious, but it informs how the entire operation works. If permanent damage is inflicted, or data is lost, then what incentive is there to pay the people who did it? It's a tough engineering challenge to compromise a wide array of heterogeneous technical assets and make unlocking an environment simple and non-destructive. For this reason, ransomware groups are organized and the tools they use are tested.

Ransomware groups are known for employing customer-service lines that will walk you through each step of the decryption process from buying the Bitcoin, to transferring the cryptocurrency, to decrypting machines (in your native language, too). After all, they want you to know that paying them will get your data back.

Otherwise, ransomware does not differ greatly from other kinds of attacks from a purely technical perspective. Attackers need to find an initial entry point, pivot around the environment, escalate privileges, and detonate their payloads – all familiar steps in the exploit process.

MOVES: BRAZEN

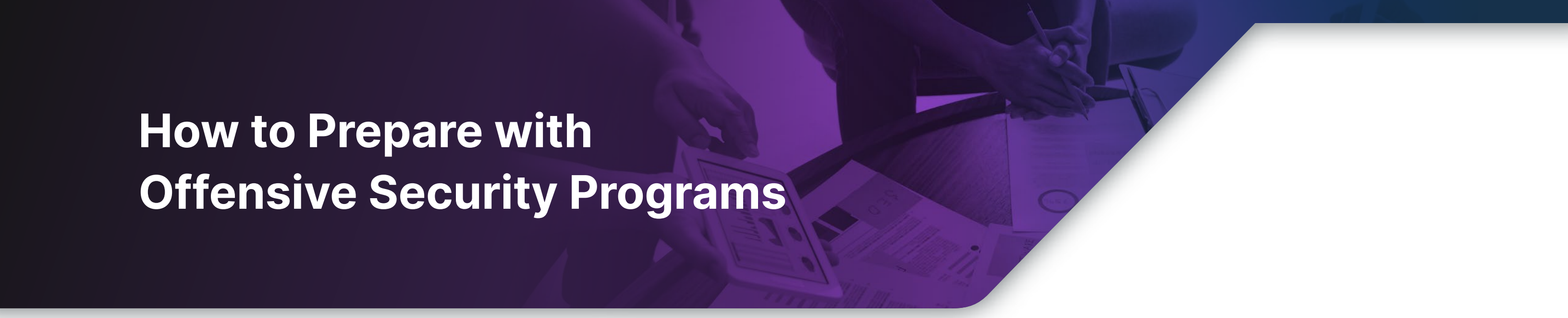
Ransom Threats Can Quickly Escalate Into Blackmail and Extortion.
Ransomware attackers typically operate in countries outside of Western jurisdictional boundaries, so they can be more aggressive than other kinds of threat actors. They care about getting caught only to the extent that it will cause them to lose money by being kicked out of the network before infecting as many machines as possible. After all, even if you did catch them and thwart the attack, they'll just move on to the next target. No jail time, no big deal. This means that they will pivot around a network to try and scoop up as many assets as possible quickly. Each uncompromised machine is a potential backup server that can undermine the whole operation.

There's nothing off-limits to ransomware attackers. After gaining access to their victim's network, some ransomware attackers steal sensitive data before launching the encryption routine. To increase the pressure on the victim to pay quickly, the attackers may threaten to release the sensitive information if the ransom is not met or paid in a timely fashion. So, while backups may nullify the need for a decryptor, they cannot stop an attacker from blackmailing their victim – or disclosing the sensitive data – no matter how the victim responds.

Thanks to ransomware-as-a-service, these attacks are available to a mass market with enterprise-level support operations and infrastructures. Trickbot, responsible for more than $61M in damages worldwide and at least one death, employs payroll, customer service, product management, and HR departments with aggressive recruiting practices.

THE SAD AND UGLY TRUTH:

It's Not Rocket Science.
The best way to protect against a ransomware attack is no secret. And it's very boring. Patch applications and operating systems; enforce the principle of least privilege everywhere (e.g., protect access with strong passwords you don't share; disable unnecessary ports, protocols, and apps; segment networks; use encryption; etc.), and run a regular backup and system recovery program. The only difference now? The buzzword the market uses: cyber hygiene.



How to Prepare with Offensive Security Programs

The most mature security programs are those that include a healthy balance of defensive and offensive security tactics. Despite the tired 'cloak and dagger' stereotype offensive security seems unable to shed, these practices can truly shine light into darkness.

By using the insights gained from an offensive security program, you'll hone your defenses in ways that are informed by real-world data. An offensive security program will identify where your business is vulnerable to a ransomware attack, demonstrate and document how it's possible an attacker would execute one, and make pointed recommendations on how to address any gaps found.

PRO-TIP

Start at the End. It sounds like a riddle, doesn't it? What we mean is start your ransomware readiness assessment by determining what your end goals are. For example, consider which of the following take priority (this will likely change as you learn more about your environment):

Vulnerability Discovery
Are you interested in discovering how many vulnerabilities are currently exposed to ransomware attackers?

Asset Management
Do you need greater visibility into the assets on your network and how data flows across the environment to better assess where your network might be vulnerable to a ransomware attack?

OR

Detection and Response Improvement
Do you want to know how well your organization can detect and respond to an active ransomware attack?

Team Cohesion
Do you want to ensure your cross-functional teams are ready to respond if (or when) a ransomware disaster strikes – from detection to response to public disclosure?

Knowing what your desired outcomes are as well as what you will do with the lessons learned is essential. Ensure that all stakeholders are involved in the decision making, planning, and execution.

The following table includes five ways to assess and/or improve your ransomware readiness. Use the questions we started with as guideposts to land on your desired outcomes and then map those against the approaches outlined in the table below.

RANSOMWARE READINESS PROGRAMS

SIMULATION PROGRAM & GOALS	WHAT TO EXPECT	WHO PARTICIPATES	PRO-TIP
External Penetration Testing Identify exploitable vulnerabilities and weaknesses in the perimeter.	A report of vulnerabilities to patch, systems to decommission, network diagrams, and open ports to disable (e.g., RDP).	Penetration testing service provider with no organizational involvement (or some, negotiated in advance).	Prepare your team for the test by notifying all stakeholders (to avoid setting off any unnecessary alarms).
Internal Penetration Testing Discover the most likely vulnerabilities, attack paths, and exploit chains that an internal threat actor could leverage to gain access to your sensitive data and critical functionality.	A report with guidance on how to properly segment your network, implement stronger authentication, and mitigate their discovered vulnerabilities.	Penetration testing service provider with minimal organizational involvement negotiated in advance.	Prepare your team for the test by notifying all stakeholders (to avoid setting off any unnecessary alarms).
Red Teams Measure the efficacy of people, processes, and technology in real-world scenarios.	Detailed attack graphs and architecture diagrams. An assessment report with technical findings, timelines, and remediation recommendations.	Offensive security service provider actively planning and collaborating with the organization.	Base scenarios on specific outcomes; an 'assumed breach' approach to a red team engagement will often save time and money with identical outcomes.
Purple Teams Test and improve people, processes, and technology with red teams and blue teams working together.	A purple team is very similar to a red team but simply conducted with full knowledge of both the attackers and defenders, making it a great learning opportunity.	Offensive security service provider actively planning and collaborating with the organization.	If you've never conducted a red team engagement, a purple team can be a great first step and offers a lighter introduction to adversary simulation.
Tabletop Exercises Anticipate, assess, and respond to operational and strategic security risks in a facilitated group setting.	A paper-based (i.e., tabletop) exercise with key stake holders and an after-action report detailing key takeaways.	Security services provider facilitates with cross-functional team participation.	Establish the strategic goals with clarity and include as much cross-department representation as possible. After all, a ransomware attack will touch the entire organization.

TOP FIVE RANSOMWARE SIMULATION DO'S

1 – Get Clarity on Your Goals.

Before engaging an outside firm, first gather your team to discuss the following critical questions. Document your answers once you reach consensus.

- Why are we doing a ransomware simulation program?
- What are we most concerned about in our environment?
- What are the worst-case scenarios when it comes to ransomware?
- How do we plan on using the results of these programs?
- Do we have the capacity to implement the changes needed to address any gaps we find? If not, where will we find the resources and what are the next steps?

2 – Determine if You'll Pay the Ransom in the Event of a Real Attack.

This is the most important question the business leadership – in consultation with counsel – must answer. Law enforcement agencies and cybersecurity industry experts agree that *not* paying the ransom is the best option.

At the same time, if an organization decides it's in their best interest to pay – despite the risk that the data may be unrecoverable – it's important to establish legal and payment arrangements ahead of time. Whatever the decision, teams are best served to do this type of preparation now rather than later.

Additionally, consider cybersecurity insurance programs. At the end of the day, ransomware can be seen as a monetary threat to your business, just as fire and flood might be. While a certain due diligence should be paid to prevention, it may also be prudent to purchase insurance against the threat. Of course, this is a complicated cost-benefit analysis that only you can make for yourself.

3 – Establish the Rules of Engagement Upfront.

There should be clear cut rules of engagement – whether it's a penetration test or a red team – on when, how, and if they get involved in the simulation exercise. Know what your goals are internally, and then clarify these goals and negotiate the plan with your penetration testing team before the simulation begins.

For example, assume you decide to separate your production environment from a test environment (or better yet already have this setup in place). Running the simulation against your test environment will avoid any downtime risk. That said, what you gain in risk avoidance, you lose in visibility into the real-world risks facing your business operations.

4 – Consider the Escalation Path – Where It Begins and Ends.

Ransomware simulation programs are designed to escalate and will likely branch off into unexpected domains and directions. To prepare for this, decide how far you'll let the exercise escalate. What are the triggers? Your assessment team can also guide you on the best escalation procedures for your organization size, geography, and industry.

5 – Establish Clear and Documented Communication Lines – Before, During, and After the Exercise.

Other than those team members who might not be 'read in' to the program, frequent team communication on the roles, responsibilities, and rules of engagement is essential. Miscommunication while conducting regular business can be costly, but during a ransomware simulation it can expose companies to unnecessary legal and financial risk.

Your program should have a solid foundation, IF all team members:

- Understand what is expected of them.
- Know when, where, and how to execute on the mission, including who to ask when they have pressing questions.

TOP FIVE RANSOMWARE SIMULATION DONT'S

1 – It's Not a 'One and Done.'

As with everything in life, success involves consistence and persistence. Readiness isn't a thing you 'achieve,' it's a process you must constantly engage in. However, what ransomware simulations offer is truly valuable insight into where your security controls, policies, and practices can be fine-tuned for preventative defense. After all, preventing a ransomware attack is the best protection. Just remember that it does mean a commitment to a continuous approach and iterative security policy enhancement.

2 – Don't Limit Yourself by Treating This as a Purely Technical Endeavor.

Ransomware attacks are existential crisis moments for any company – large or small – across every industry. As such, treat it by addressing risk via a 'whole company' point-of-view. Allow the assessment to test your business processes as much as your technical ones. A cyber attacker doesn't limit themselves to only probing technical vulnerabilities, particularly when hunting for large game.

3 – Don't Forget the Question of IP Allow-listing (or Disabling a WAF).

IP allow-listing is the practice of adding the IP address of the pen tester to an allow-list to avoid auto-blocking or setting off unnecessary alerts (disabling a WAF may also be required). This preparation work can lead to faster discovery of more high priority risks. Rather than waste time on the exhaustive 'easy stuff,' a penetration tester can spend more time on probing higher value, at-risk assets – the ones your attacker targets.

At the same time, using an allow-list for a red team exercise would not be recommended. It's ultimately your decision at the end of the day, but what we've found is that without allow-listing for a pen test, the assessment will test your pen testers' abilities, rather than expose your organization's biggest risks.

4 – Don’t Overthink Red Team Tactics.

During a Red Team exercise, uncertainty rules the day. Embrace it, and make sure you approach each new situation or discovery with multiple strategies. A primary goal of a Red Team is to build muscle memory into your organization’s response procedures, because a loss of control will increase the chance of failure.

To avoid getting stuck, follow the **PACE principle of planning**: have a **Primary, Alternative, Contingency, and Emergency plan**. Like Mike Tyson says, “Everyone has a plan until they get punched in the face.”

5 – Don’t Neglect to Train Your Employees.

Security awareness programs are one of the most critical ways to combat any cybersecurity issue, particularly when so many workers are remote and are connecting to corporate data and apps via public networks using a variety of devices. It’s no surprise that ransomware attacks increased **148% during the initial stages of the COVID pandemic.**

As part of a comprehensive security awareness training program, establish a culture of trust with your employees so that they are encouraged to speak up (e.g., ‘see something, say something’). If employees are too afraid to admit they might have exposed the company to a risk like ransomware, any outbreak will likely spread further and faster and complicate recovery efforts.

OPEN-SOURCE TOOLS & FRAMEWORKS

There are a lot of valuable security tools and frameworks available in the open-source community. The following two tables list some of the most referenced open-source tools and frameworks typically used by penetration testers, and red and purple teamers.

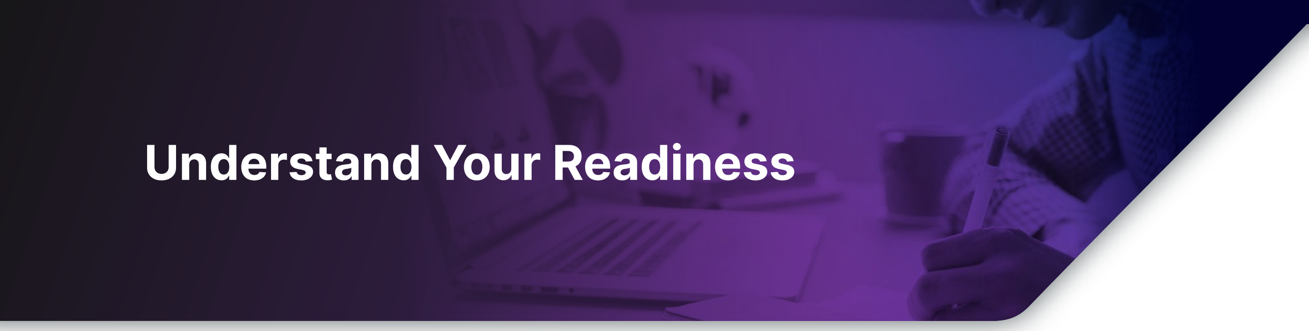
Whether you decide to build your own offensive security team in-house or outsource to an offensive security services provider, use this reference to broaden your understanding of the use cases, capabilities, and deployment considerations involved in setting up a ransomware simulation. **Chances are that the provider you decide to go with may be a contributor to one or more of the following tools and frameworks.**

OPEN-SOURCE TOOLS FOR RANSOMWARE READINESS

OPEN-SOURCE TOOL	PROS	CONS
Atomic Red Team From Red Canary **Ransom Readiness Use Case:** Run basic TTPs on your systems to test detection capabilities for ransomware in your environment.	Simple to run and offers a wide breadth of TTPs and detections.	Testing is conducted in a vacuum, doesn't always reflect realistic outcomes and lacks social engineering component.
VECTR from Security Risk Advisors **Ransom Readiness Use Case:** Similar to Atomic Red Team, VECTR facilitates tracking of red and blue team testing activities to measure detection and prevention capabilities across different attack scenarios, including ransomware.	Extensive reporting and heatmaps help pinpoint gaps in defenses and raise internal awareness.	May require advanced skills as it can be cumbersome and complex to configure and implement.
BloodHound **Ransom Readiness Use Case:** Using graph theory, BloodHound reveals the hidden (often unintended) relationships in AD environments. Both blue and red teams can use BloodHound to easily gain a deeper understanding of privilege relationships in an Active Directory environment - an essential step in preparing for and protecting against ransomware attacks.	Works quickly to analyze, expose, and report on the biggest privilege and permissions risks—a rich target for ransomware attackers.	Complex but not difficult—relies on advanced AD understanding and is limited to Active Directory shops.
Caldera from MITRE **Ransom Readiness Use Case:** Built on top of MITRE ATT&CK, Caldera is a cybersecurity framework designed to easily automate adversary emulation, assist manual red teams, and automate incident response. All of these are critical functions to exercise to determine your ransomware readiness status.	Works well for organizations heavily invested in MITRE ATT&CK and offers a healthy set of plugins for reporting and other functionality.	Not totally complete, still involves some heavy lifting on set-up and configuration.
Sliver from Bishop Fox **Ransom Readiness Use Case:** To simulate a ransomware attack, penetration testers, red teams, blue teams, and purple teams use SLIVER to set up Command-and-Control (C2) systems to run on virtually any architecture, and securely manage connections through a central server.	Powerful tool for replicating adversary architecture, well-supported and documented.	Advanced and requires networking expertise (much like a scalpel is appropriate for a surgeon... not just anyone).

OPEN-SOURCE FRAMEWORKS FOR RANSOMWARE READINESS

OPEN-SOURCE FRAMEWORK	PROS	CONS
Scythe **Ransom Readiness Use Case:** Use this Purple Team Exercise Framework (PTEF) to establish a formal Purple Team Program and perform adversary emulations as Purple Team Exercises and/or Continuous Purple Teaming Operations.	Can jumpstart your own purple team program quickly.	Self-directed and as such may require a heavy lift.
Ransomware Readiness Assessment (RRA) from US CISA (Cybersecurity and Infrastructure Security Agency) **Ransom Readiness Use Case:** Use this security audit self-assessment tool to understand how well you're equipped to defend against and recover from ransomware attacks targeting your information technology (IT), operational technology (OT), or industrial control system (ICS) assets.	Good starting point for a self-assessment that covers a wide range of control areas.	Typical for self-assessments, involves a lot of manual work.
ATT&CK from MITRE **Ransom Readiness Use Case:** Use this knowledge base of adversary tactics and techniques as a foundation to analyze ransomware attack methods and model ransomware attack scenarios.	A complete reference, 'zoology of attacks', and good way of organizing attacks.	Not designed to assist with preventive detection or identification.
MITRE Engage **Ransom Readiness Use Case:** Use this knowledge base of active defense to capture and organize lessons learned about active defense and adversary engagement. Derived from over 10 years of adversary engagement experience, it can help both CISOs and practitioners better prepare to defend against ransomware and other attacks.	Easy way to view mappings and connections among ransomware adversaries and their tactics.	Still in development stages, incomplete.



Understand Your Readiness

At the start of this eBook, we suggested that starting with the end goal in mind is the best recommendation for deciding which offensive security program will work best for your organization. It is also a good idea for gauging your organization's level of ransomware readiness.

To surface your goals, we posed pointed questions across the following key goal categories: vulnerability discovery, asset management, detection and response improvement, and team cohesion. We'll use these same goal categories in the following checklist.

VULNERABILITY DISCOVERY

When Was the Last Time You Ran a Penetration Test Internally? How About Externally?

WHY THIS IS IMPORTANT:
Having a baseline understanding of your technical exposures (internally and externally) – not to mention progress over time – provides a good picture into your current exposure.

HOW TO INTERPRET 'READINESS' FROM THE ANSWER:
The more frequent your penetration testing program is, the more likely it provides an accurate picture of your security posture. In other words, you're nowhere near 'ransomware ready' if you haven't run a single assessment against your environment.

What Were the Results from Previous Assessments? How Many High and Critical Severity Findings Did You Identify?

WHY THIS IS IMPORTANT:
Pay attention to the content of the results over time. Even though a single finding may be severe and require attention, is it indicative of a larger issue or is it a one-off problem? Are the same sorts of issues found year-after-year?

HOW TO INTERPRET 'READINESS' FROM THE ANSWER:
Make sure that you're improving security over time. Make new mistakes. Individual security issues come and go, but as long as they don't present persistent patterns of vulnerabilities then you're on the right track.

How, When, and Where Have You Implemented Any Recommended Fixes?

WHY THIS IS IMPORTANT:
Basic cyber hygiene practices like implementing patches, removing unnecessary privileges, and reconfiguring insecure systems are the best ways to reduce ransomware risk.

HOW TO INTERPRET 'READINESS' FROM THE ANSWER:
The more advanced your organization is at maintaining basic hygiene across your critical assets (and measuring this over time) the better.

ASSET MANAGEMENT

Which Assets Do You Anticipate are the Most at Risk to a Ransomware Attack? Do You Have Visibility Across the Entirety of Your Attack Surface?

WHY THIS IS IMPORTANT:
You can't secure a server that you don't know exists. Fighting back against shadow IT isn't just good for your IT department's sanity, it's also good security.

HOW TO INTERPRET 'READINESS' FROM THE ANSWER:
When your penetration testing team asks for the company's external exposure, do you have an up-to-date comprehensive answer?

DETECTION AND RESPONSE IMPROVEMENT

When Was the Last Time You Tested Your Ability to Detect Specific TTPs? What Did You Learn and What Did You Do About What You Discovered?

WHY THIS IS IMPORTANT:
Having a baseline documented understanding of your detection capability (including speed of detection across varied samples) can provide a quick snapshot into areas that may need additional investment, fine-tuning alerts, or adjusting policy.

HOW TO INTERPRET 'READINESS' FROM THE ANSWER:
Organizations that continually assess and improve their threat detection and response capabilities will be more ransomware ready with each iterative exercise.

What are the Specific Steps You'll Take Once You Detect Ransomware in Your Environment? Is Your Goal to Isolate and Recover Without Paying Ransom or Do You Have Other Goals in Mind When/if an Attack Happens?

WHY THIS IS IMPORTANT:
A plan A and a plan B are both necessary ingredients for ransomware readiness (and in fact, for any cybersecurity crisis). Not everyone will agree, and that's best to find out now, before the fan gets hit by you-know-what.

HOW TO INTERPRET 'READINESS' FROM THE ANSWER:
This is a litmus test question. It's a lofty goal but teams that achieve clarity, consensus, and communication on what to do, how to do it, and who does what and when are closer to readiness.

TEAM COHESION

How Prepared are You to Take Time Away from Regular Business to Sit in a Conference Room and Test Your Ransomware Readiness?

WHY THIS IS IMPORTANT:
Tabletop exercises are one of the best ways to assess ransomware readiness and establish a go-forward plan to address weaknesses – on both the technical and business side. Yet they require valuable time, attention, and input from department heads and some of their team members – so gauge interest and set expectations early on.

HOW TO INTERPRET 'READINESS' FROM THE RESULTS:
The more interest you can gain the higher up in the organization hierarchy, the more likely you're already high up on the ransomware ready scale (and ready for even more improvement).

About Bishop Fox

Bishop Fox is recognized as the leading authority in offensive security, providing solutions ranging from continuous penetration testing, red teaming, and attack surface management to product, cloud, and application security assessments.

Over the past 16 years, we've worked with more than 25% of the Fortune 100, 8 of the top 10 global tech companies, and hundreds of other organizations to improve their security. Our award-winning Cosmos platform was named Best Emerging Technology in the 2021 SC Media Awards and our offerings are consistently ranked as "world class" in customer experience surveys.

Security isn't just a job to us. We do this because we love it — and because we're committed to the common good. In fact, we have authored 15 open-source tools, shared groundbreaking research, and published more than 50 security advisories in the last 5 years.

Cosmos

Cosmos proactively defends dynamic attack surfaces by combining advanced technology, automation, and expert-driven testing to continuously identify and remediate high-risk exposures before attackers even know they exist.

Leveraging a proprietary asset discovery and exposure reconnaissance engine, Cosmos continuously discovers and maps your ever-changing attack surface and identifies dangerous vulnerabilities targeted by attackers.

Acting as an extension of your security team, our operators provide deep insights into findings, deliver real-time answers to pressing questions, and conduct on-demand retesting to validate remediation procedures and accelerate the closure of attack windows.

Consulting Services

Ransomware Simulations

Putting your ransomware playbook to the ultimate test, Bishop Fox's security experts covertly execute ransomware attacks to measure the performance of your defenses, your ability to detect malicious activity commonly seen, and the efficacy of your security team's processes and communications.

Red Teaming

We utilize advanced offensive tools and tactics that mimic real-world adversaries to identify exploitable weaknesses in your organization while stress testing your incident responders and their playbooks for handling active, persistent attackers.

Internal Penetration Testing

By simulating an attacker who has gained access to the internal network, we locate the most likely vulnerabilities, attack paths, and exploit chains an internal threat actor would leverage to gain access to sensitive data and critical systems.

CONNECT WITH US

Get started today.

Are you ready to start "defending forward"? Get in touch with our offensive security experts today to explore solutions that meet your unique business needs.

Request a Meeting

Explore Cosmos

8240 S. Kyrene Rd. • Tempe, AZ 85284
480.621.8967
hello@bishopfox.com • bishopfox.com