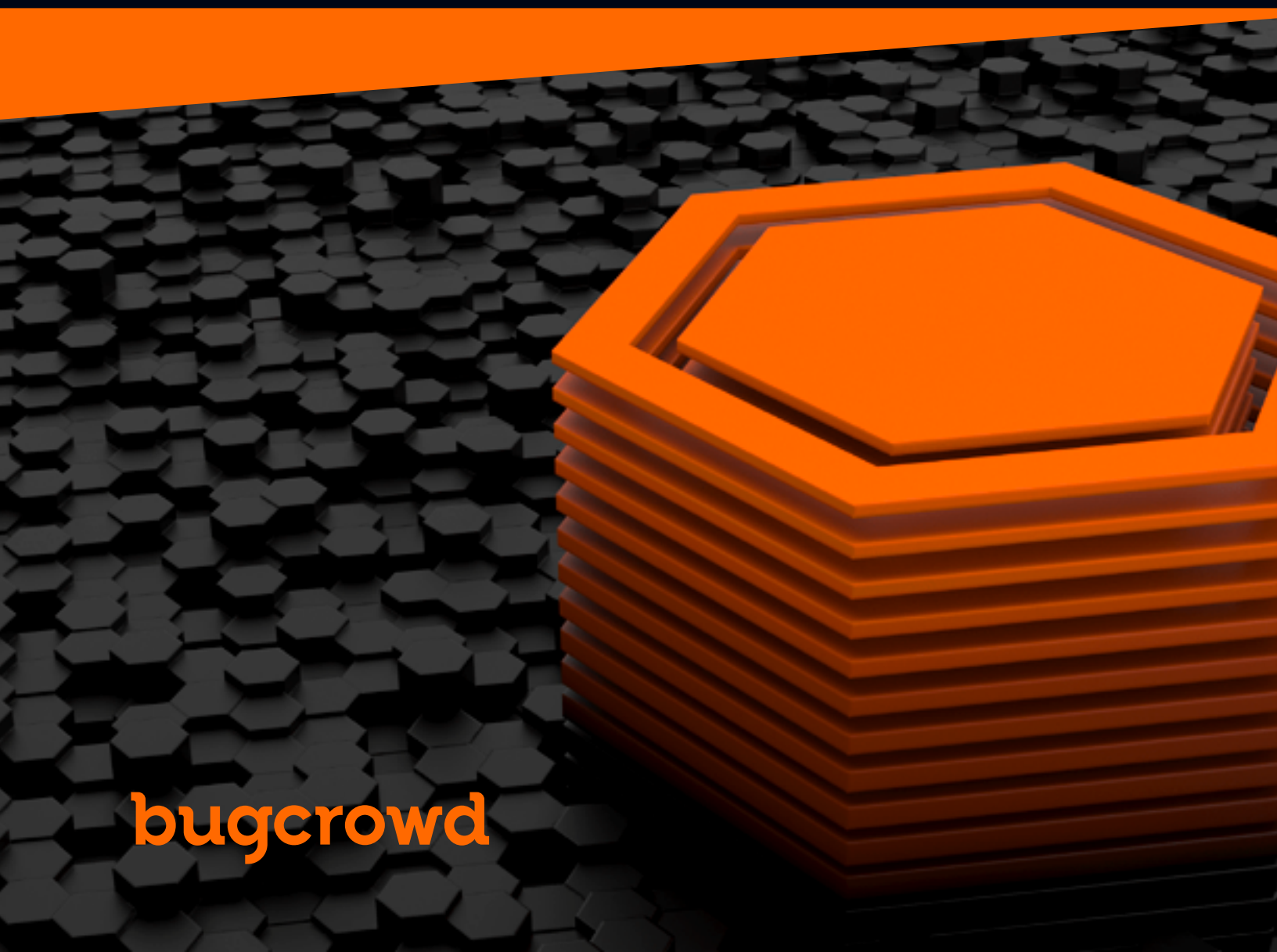
THE ULTIMATE GUIDE TO

Cybersecurity Risk Management



bugcrowd

TABLE OF CONTENTS

INTRODUCTION

Imagine you are considering insurance policies, such as health insurance, auto insurance, or home insurance. All of these policies are ways to help protect yourself against losses like flood damage or repairs on a fender-bender. Purchasing these insurance policies does not guarantee you safe from all potential losses, but it does provide a layer of protection and more peace of mind.

Cybersecurity risk management is a little bit like an insurance policy. In this guide, we'll define cybersecurity risk management, talk more about the importance of establishing a company culture that respects internal security practices, and provide tips to help you get started with cybersecurity risk management.

WHAT IS CYBERSECURITY RISK MANAGEMENT?

Cybersecurity risk management is the process of determining the risks that your organization is likely to face and then prioritizing and selecting the security control technologies, best practices, and policies to reduce or mitigate these risks.

Just like how no amount of auto insurance can guarantee you won't get into a car accident, no organization can completely eliminate every vulnerability in their system or block all cyberattacks. Cybersecurity risk management helps organizations **address the risks that are of most potential impact** on their operations.

The better your information about the threats most likely to impact your organization and the vulnerabilities that exist in your infrastructure, the better you can **reduce risk** and optimize outcomes in the event of a security incident.

ESTABLISHING A PRO-SECURITY CULTURE

Within organizations, security teams are often seen as the "Department of No." The information security function has gained a reputation for sometimes blocking activities in support of the digital transformation. When the risk is assessed and understood, chief information security officers (CISOs) can move from saying no to driving the business forward.

The key is to have a comprehensive assessment of risk and to understand the vulnerabilities that any architectural deployment and changes present. An IDC/ CapGemini Study, The Modern, Connected CISO[1] notes that "CISOs are now involved in significant business decisions, with 25% of business executives perceiving CISOs as proactively enabling digital transformation, a key business goal for 895 of organizations surveyed by IDC."

The establishment of a **cybersecurity risk management culture** helps keep employees in step with the defined governance. Once risk is understood, priorities can be managed and the organization can move forward more quickly to implement positive and necessary changes.

In contrast, moving forward too quickly without understanding the risk and vulnerabilities you face can expose the organization to the **massive damage of a successful cyberattack.** The solution is **more employee participation and support for security-aware culture**. Training is an essential component of establishing and promoting a security-aware culture. The return on investment for doing this can be significant. A successful cyberattack can cost millions in damage to an organization's brand, their reputation, damage to the customer experience, loss of revenue, reduction in profitability, and impact key operations.

> Best practice risk management should include technology, processes, and people

Team members should participate in **regular and continuous cybersecurity training**. All team members should understand how to act to minimize cyber risks to the organization. Cyber risks that employees can reduce through additional training include susceptibility to social engineering, phishing, and accidentally or intentionally created vulnerabilities.

Nobody in the organization wants to be the "Department of No." However, the potential financial and reputational damage of a successful cyberattack means it is crucial to enforce your organization's cybersecurity policies, even if that means you're occasionally seen as the "bad guy."

[1] https://securityboulevard.com/2019/01/information-security-no-longer-the-department-of-no/

THE SHIFT TO REMOTE WORK

Security policies must be enforced rigorously across your organization for any individual that has access to digital assets. This enforcement must also extend to external partners and work from anywhere (WFA) employees.

The rapid move to WFA during the pandemic has left many organizations exposed to a far **greater number of risks and vulnerabilities** than ever before. WFA enables remote workers to access enterprise resources from a wide variety of endpoints, both personal and company-provided. These may include laptops as well as mobile devices. The cybersecurity "stack" and the procedures that are used within the enterprise generally don't support this WFA environment as they were designed primarily to protect the on-premise employees. Most of the new vulnerabilities brought by WFA are unknown to their information technology and security operations teams, or the potential impact is being underestimated and perhaps ignored. All of this adds tremendously to the cybersecurity risk these organizations now face.

In today's environment, many basic cybersecurity policies and capabilities are becoming more essential.

EXAMPLES OF **IMPORTANT POLICIES AND CAPABILITIES:**

- Automate your policy execution and enforcement
- Move authentication as close to the resource, system, service, or data being accessed. A strategy for Zero Trust will help reduce risk in your organization
- Two-factor authentication should ideally be integrated in your security policies
- Understand how you will assess risk and make policy decisions for properly authenticated employees and partners wanting access to organizational resources from personal tablets, laptops, and mobile devices that may be utilizing public or home networks

5 TIPS TO BETTER RISK MANAGEMENT

Whether you're just starting out with cybersecurity risk management or a seasoned veteran, these tips will help you better **protect your organization** from cyberattacks.

1. UTILIZE A CYBERSECURITY FRAMEWORK

Cybersecurity frameworks such as the **ISO/IEC 27001/27002** address business risk and help improve overall cyberdefense. According to a survey by Dimensional Research, **84% of organizations in the U.S. already use some type of security framework**. 44% of the respondents report using more than one security framework.

OTHER IMPORTANT CYBERSECURITY FRAMEWORKS INCLUDE:

- **National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)** provides excellent guidance to understanding the necessary activities to address and reduce risk
- **The Center for Internet Security (CIS) Critical Security Controls** which includes 20 critical security controls recommended as best practices to reduce the the risk of successful cyberattack
- **The Payment Card Industry Data Security Standard (PCI DSS)** which provides detailed direction on the best practices to process credit and debit card information

2. DEFINE AN ONGOING RISK ASSESSMENT PROCESS

A risk assessment process should show how the organization will **prepare** for risk assessment, **conduct** the risk assessment, **communicate** key risk assessment results across various team members within the organization, and regularly **maintain** the risk assessment process over time.

PREPARATION FOR A RISK ASSESSMENT INCLUDES:

- Carefully defining the scope and any key assumptions or limitations with the assessment
- Identifying the sources of information to be used to conduct the assessment
- Define the risk calculations and analytics approach to be used during the assessment
- Structure your risk assessment to map to the compliance regulations that impact your organization—these regulations have varying requirements for risk assessment and reporting

https://www.tenable.com/whitepapers/trends-in-security-framework-adoption

THE ONGOING RISK ASSESSMENT PROCESS SHOULD INCLUDE:

- An overview of the environment in which risk-based decisions are done
- An understanding of how the organization will assess risk. Per NIST, the risk is defined as the likelihood of a given threat event exploiting the vulnerability of an asset and the resulting impact of the occurrence of the threat event
- A plan and process for how the organization will respond to risk once that risk is determined based upon the outcome of a risk assessment
- The process for how the organization will monitor risk over time
- The form and structure of documentation and the output from the risk assessment process

Your information technology systems and networks are continually changing. Software applications are being updated and new employees are entering your organization.

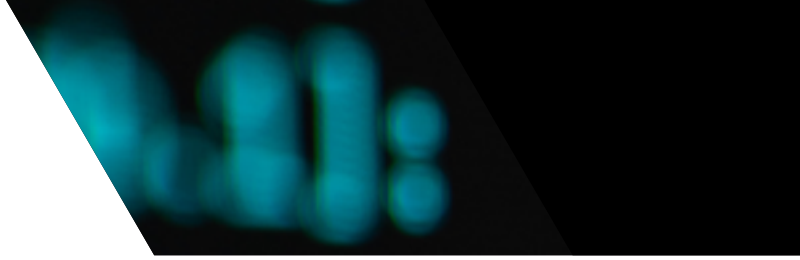
> New risks will continually be found and even those previously resolved may be reborn by leveraging new vulnerabilities

New vulnerabilities appear all of the time.

3. USE THREAT INTELLIGENCE TO BETTER PRIORITIZE RISKS FOR YOUR ORGANIZATION

Threat intelligence provides very **timely information** on the current threats most likely to impact your organization, your geographic location, and your industry. Threat intelligence can enable you to make important adjustments to your current risk assessment to **avoid newly emerging and dangerous threats**. 43% of surveyed companies by SC Media noted that they expect threat intelligence to bring early warning of new threats or tactics, 9% felt that threat intelligence brought benefits such as aiding in incident event investigation, and 23% felt that threat intelligence was useful in uncovering new exploits or vulnerabilities affecting technologies your organization may use.

Threat intelligence data is collected, reviewed, and analyzed so that security and information team members can make **faster data-driven decisions** about threats that may impact the organization. Threat intelligence includes data about threat groups and ongoing attacks. Threat intelligence data may include specific attacker behavior such as their tactics, techniques, and procedures, the attack vectors they use, and known indicators of compromise.



4. LEVERAGE PENETRATION TESTING FOR THE BEST DATA ON VULNERABILITY AND EXPOSURE

Penetration testing is the process of hacking into your own system and network to identify and expose as many vulnerabilities as you possibly can, from multiple vantage points. Penetration testing is performed by **"ethical hackers" or security researchers** who are highly specialized. Penetration testers search for vulnerabilities with full knowledge and authorization from the client. When protecting your organization from malicious hackers, you want to think like one so as to anticipate and protect where they might strike your organization.

This brings up the relevance of vulnerability scanners. Although useful, vulnerability scanners are not enough and miss newly discovered vulnerabilities. Sometimes the vulnerabilities are too complex to be found by an automated tool. False positives are a regular event with these scanners, especially with a large infrastructure. **Human ingenuity** is key when testing for vulnerabilities. When many think about penetration testing, it is often considered through the lense of compliance regulations. You may be surprised to learn that **compliance is no longer the number one reason for penetration testing**. In a recent survey, Bugcrowd found that while 55% of respondents cited compliance as one of their reasons for testing, only 16% test purely for compliance purposes. Meanwhile, 61% of respondents cited best practices and reducing risk as a reason for testing. This shows an **increased commitment to penetration testing** as part of a wider cybersecurity risk management strategy, as well as a general focus on reducing risk.

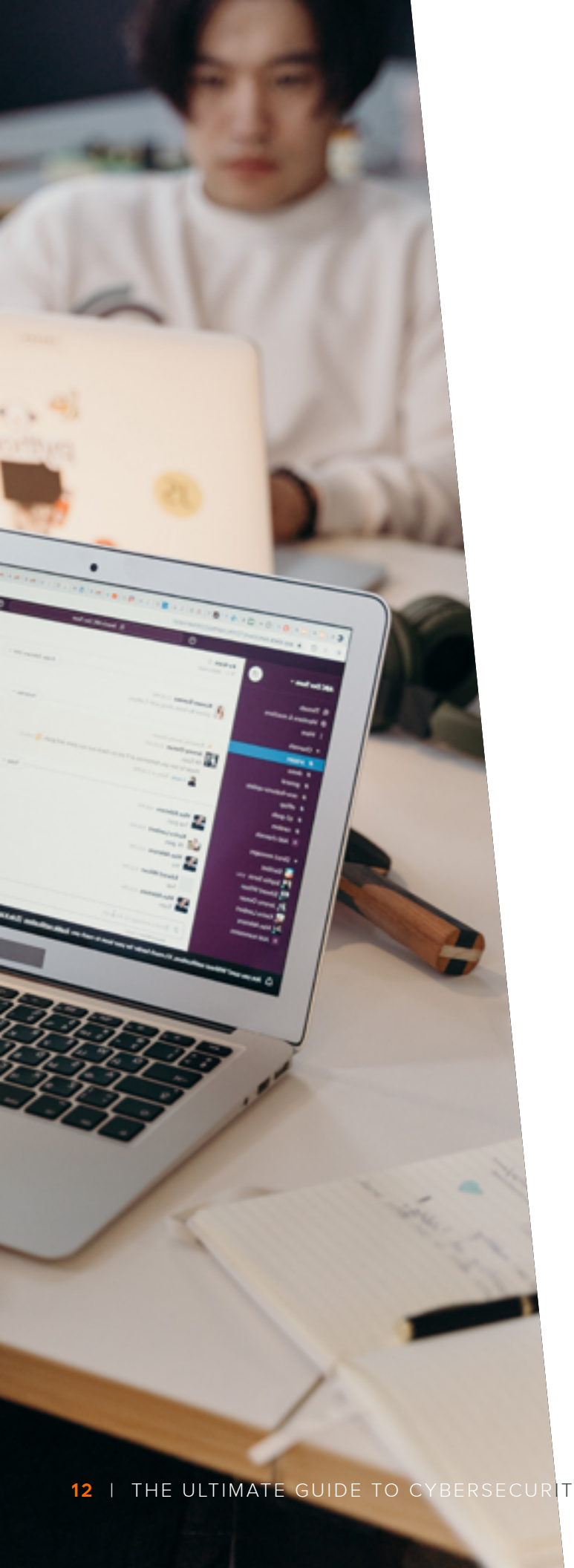
> Through penetration testing, organizations gain visibility to many vulnerabilities that might represent very significant risks to your infrastructure and organization. Regular penetration testing is essential to optimizing your cyber risk management

https://csrc.nist.gov/glossary/term/risk
https://www.recordedfuture.com/threat-intelligence-industry/

5. USE TOOL RATIONALIZATION FOR IMPROVED CYBERSECURITY ROI

Cyber risk management will help you identify performance gaps and missing coverage. You may also find unnecessarily **redundant layers in your security controls**. Once identified, security controls can be consolidated, eliminated, or reallocated within the organization. Cyber risk management can help empower this process of tool rationalization so that you can **maximize your operational cybersecurity capabilities at the lowest cost.**

Your team can set a target security posture and methodically measure your existing security infrastructure against reaching that objective. Cost can be an important part of the analysis. Every dollar spent must provide the protection that your organization expects. Some threats and identified vulnerabilities may require overlapping security controls to manage the risk and mitigate the vulnerabilities that will likely be exploited.



BUILDING A CYBERSECURITY RESPONSE PLAN

A cybersecurity incident response plan is a **playbook of instructions, processes, and procedures** to help your organization respond to a detected threat and to recover from an ongoing cyber incident. Cyber incidents that require a **rapid and well-orchestrated response** include malware detection, the theft of data, or service outages.

The purpose of a response plan is to allow your organization to respond rapidly and correctly to an adverse cybersecurity incident.

AN **ADVERSE EVENT** MAY INCLUDE:

- An apparent violation of your organization's security policy
- Attempts to gain unauthorized access to your organization's network and information resources
- Unauthorized use or modification of your organization's information technology
- Loss or breach of your organization's confidential information
- Denial of service to any of your information technology assets

LEVELING UP CYBERSECURITY RISK MANAGEMENT WITH CROWDSOURCEDSECURITY

As the amount of software and internet surface increases, vulnerabilities increase, meaning security risk increases. Luckily, the security industry is innovating constantly. Bugcrowd introduced the world to security testing performed by **the Crowd**, a collection of on-demand ethical hackers (aka security researchers) distributed across the world and connected via the Bugcrowd platform. The Crowd powering this new type of security testing consists of security researchers with diverse backgrounds, from academics with advanced degrees in India, professionals who hack as a hobby, to self-taught hackers in Idaho—all united by their ability to demonstrate tangible results in security testing. This new breed of **crowdsourced security** allows organizations to tap into expert testing at scale, provides a source of income to bright researchers outside of the formal security industry, and brings security testing up to scratch for a digital-first world. Crowdsourced security allows organizations to deploy a suite of **advanced security testing methods** while defining a scope, remuneration model, and timeline that is tailored entirely to their independent way of working.

Crowdsourced security is a powerful tool – used by leading-edge firms such as Google, Apple, and Facebook – to **decrease risk**. Crowdsourced security provides focused results to support rapid risk reduction, cost control, and lower operational overhead. Crowdsourced security supports the most critical attack surfaces: web and APIs interfaces on server/cloud, mobile, and IoT platforms.

In addition to penetration testing, which we've already discussed in this guide, let's look at some of the other different forms of crowdsourced security testing that help with cybersecurity risk management.

VULNERABILITY DISCLOSURE PROGRAMS

The first step in crowdsourced security for many organizations is establishing a Vulnerability Disclosure Program (VDP). This is a channel that invites users and members of the public to submit any vulnerabilities found in an organization's assets. Think of a VDP as a "**neighborhood watch**"—the ability for an organization to receive security feedback from anywhere to reduce the risk of a breach. A VDP requires the scope of testing and terms of engagement to be clearly defined and needs to provide communication channels that allow researchers to identify and report vulnerabilities and receive a prompt response to submissions in return.

VDPs are a fantastic tool to help organizations reduce risk. **87% of organizations with a VDP have received a critical or high priority vulnerability submitted through their VDP**. By allowing for the communication of vulnerabilities found in the routine use or testing of externally-facing products and services, organizations can greatly expand their risk reduction with minimal disruption to existing security and production lifecycles. VDPs are a great way to dip your toes into crowdsourced security as part of a greater cybersecurity risk management strategy.

BUG BOUNTY PROGRAMS

Greater internet connectivity meant more threats for companies at first, as attackers seek to probe and compromise connected assets. There was **50x more online data in 2020 than in 2016.** On top of that, **the dark web is 5000x bigger than the surface web** and is often used by a growing cybercriminal community to trade tools and tactics. These numbers show us that the risk of compromise has never been higher.

This increased risk has also increased innovation. In the last decade, companies have been able to leverage this connectivity to boost their defenses using crowdsourced security in the form of a bug bounty program. This is a lot like a VDP, but in addition to social recognition, finders are rewarded financially. This has the effect of motivating researchers, and the task of finding vulnerabilities and proposing fixes is taken up by ethical hackers working for individual cash, or cash equivalent rewards.

Companies can implement bounty programs independently or through a partner such as Bugcrowd. Working with a partner removes the need to vet hackers, triage bug submission, and distribute rewards. The topic is one we have a lot of opinions on, so we would recommend checking out the Ultimate Guide to Bug Bounty or our 2021 State of Crowdsourced Security to learn more.

ATTACK SURFACE MANAGEMENT

While penetration tests are useful for their specific scope, sometimes there is value in going the opposite direction and taking a **broad approach to security testing**. Attack surface management involves giving crowdsourced security researchers license to use reconnaissance skills and tools to find remote and forgotten assets that a company has lost track of.

Locating these "**shadow IT**" assets uses crowdsourced security testing to identify unknowns and reduce risk that the organization was not previously aware of. It's important to remember that just because an asset is unknown to your organization, it doesn't mean it's lost to everyone. Gartner says that **one third of successful attacks are against unknown or unprioritized assets**. Hackers recognize that unknown attack surface is a rich vein of vulnerabilities.

Although attack surface management is such a key element of a cybersecurity risk management strategy, it's often not prioritized— **two thirds of organizations say attack surface management is getting more difficult**. You can learn more about this relatively new crowdsourced approach in The Ultimate Guide to Attack Surface Management.

CONCLUSION

As the world becomes more reliant on digital technology, cybersecurity risk management is becoming a more central part of every organization's operations. Adversaries are becoming **increasingly sophisticated**, making cybersecurity risk management **crucial** to every organization's duties to customers and stakeholders.

If you are starting out your cybersecurity risk management journey using crowdsourced security, Bugcrowd would love to help.

See why hundreds of companies turn to Bugcrowd for crowdsourced security:

www.bugcrowd.com/get-started