Simplified Steps to Improve Cybersecurity

What You Haven't Thought of Will Hurt You

Embrace an Actionable Cybersecurity Maturity Model for Hybrid IT

The fight against cybercrime is on, and it is a constant and ever-changing battle. In the past two years, more than half of all organizations have reported a significant disruption due to cybersecurity incidents,[1] and in the first half of 2020, there were over 600 significant data breaches.[2] One recent study found that the average cost of a data breach in the U.S. was an astonishing $8.6 million.[3] No matter the size or type of an organization, even the smallest loss or theft of critical data can lead to irreparable damage to the organization's bottom line and reputation.

Pandemic or not, the litany of cyberattack schemes is long and growing. When millions of workers moved their laptops from their offices to their kitchen tables in 2020, opportunities for cyberattacks on inadequately secured networks multiplied exponentially. In fact, there has been a 148% rise in ransomware attacks that relate specifically to COVID-19 scams.[4] A troubling 86% of information security professionals say that the most common attack types were on the rise during COVID-19.[5] As Charles Henderson, the head of IBM's X-Force Red security team put it, "Working from home is going to be a long-lasting reality within many organizations, and the security assumptions we once relied on in our traditional offices may not be enough as our workforce transitions to new, less controlled surroundings."[6]

The chaos inflicted by supply chain and ransomware attacks and their frequency increase has made them especially newsworthy. However, any cyberattack can potentially inflict substantial damage. Smaller organizations with between 500 and 1,000 employees incurred an average cost of $2.65 million, or $3,533 per employee, for a single incident. Organizations of this size experience higher costs relative to their size than larger organizations, and that can hamper their ability to recover financially from an incident.[3]

With this much at stake every day, ignoring cybersecurity is dangerous, and doing so won't make the risks disappear or avoid the costs. An example of the increased risk and changing environment is the latest U.S. Treasury communication that organizations may be prosecuted for paying ransoms to known bad actors.[7] All in all, current defenses may or may not be adequate or configured as needed, and untrained or unaware employees can create or exacerbate a bad situation. The result: IT management can't risk standing still.

FLEXENTIAL®

The average ransomware payment at the beginning of 2020 was $111,605, and the average downtime caused by a ransomware attack was 15 days.[8]

THE TERRIBLE COSTS OF ONE 2019 BANK DATA BREACH [9,10]

106 Million
Customer records breached

$100 Million
Legal, customer and technology-related costs

$80 Million
U.S. Treasury Department fine

$2.78 Million
Market Capitalization drop

Creating a Path Forward

Every organization is dealing with scarce resources, but with increasing threats, an organization's goal should be to improve its cybersecurity maturity. Maturity is a lens to understand an organization's appropriate cybersecurity posture, as some organizations need more security than others.

Every organization should be on a path to cybersecurity maturity. As the journey begins, it's wise to examine the current state and ask some pivotal questions:

- What kind of expertise and talent already exist within the organization?
- Does management know its priorities or have a way to determine priorities?
- Does the organization have a cybersecurity strategy, and does it include defense in depth?
- When it comes to regulatory compliance, is the organization on offense or defense?
- Does the organization need a new certification like CMMC?
- What kinds of incidents have already happened? What were the ramifications?

After evaluating the above topics, the people in charge of cybersecurity may decide they don't want to proceed entirely on their own. External experts can bring experienced perspective and simultaneously free internal resources to focus on the organization's core mission and essential value. Either way, it's time for organizations to advance toward cybersecurity maturity.

Building a Mature Cybersecurity Program

There are nine elements in a mature cybersecurity program; each one includes people, process and technology. Defense in depth—multiple security layers—can reduce cybercrime and all types of security risks.

In 2019, two of the top five causes of security breaches among remote workers were phishing scams and unauthorized use of employee credentials. Coupled with the recent 45% increase in risky and non-compliant end-user behavior,[11] it's clear that people can be the weakest link in cybersecurity defense. However, employees can also dramatically reduce security breach risk if they learn how to avoid these types of mistakes. In addition to people, a mature cybersecurity program includes process best practices and technology tools to strengthen defenses, discover weaknesses and limit risks. The following elements combine all of these and result in an actionable cybersecurity maturity path.

Roles

Whether the security staff comprises full-time employees or a combination of internal and external specialists, it should include members with current certifications for cybersecurity, risk and compliance areas. The team needs

Ignoring cybersecurity is dangerous, and doing so won't make the risks disappear or avoid the costs.

THE 5 LEVELS OF CYBERSECURITY MATURITY

Beginning
Developing
Advancing
Effective
Proactive

THE 9 ELEMENTS OF A CYBERSECURITY PROGRAM

Roles
Risk management
Vulnerability management
IT security posture
Compliance
Penetration testing
Privacy
Incident response
Governance

CLOUD-BASED RISK IN HYBRID IT

In a recent survey, 98% of organizations said they store at least some data in the cloud, and an estimated 48% of it is considered sensitive.[12] A mature security program works across hybrid IT environments: multiple clouds, SaaS applications, on-premises and co-located environments.

to be large enough to advance cybersecurity maturity and orchestrate the regular schedule of activities, testing and assessments that sufficient cybersecurity requires. Smaller organizations can struggle the most with cybersecurity due to having a small IT staff. Still, the path to maturity demands building cyber defenses and managing and mitigating incidents. Larger organizations will likely require an entire security team, including a chief information security officer and a director of IT risk.

Risk Management

One of the first and simplest things to do on the cybersecurity maturity journey is to conduct a risk assessment and follow-on gap remediation. A risk assessment evaluates and documents the current risk posture and determines the most pressing risks and their potential impact. When performed by a third party, an external set of eyes will see things the internal team overlooks. After documenting risks in the risk register, there are four ways to respond: eliminate, mitigate, transfer or accept. When mitigating, base remediation prioritization on the highest-impact actions determined by weighing cost, time and effort. On an ongoing basis, update the risk assessment and the risk register, and track remediation action completion.

Vulnerability Management

As systems change and time goes by, vulnerabilities can appear in previously secured networks, servers and applications, including edge and IoT devices. More immature organizations will do ad hoc patching, but better defenses include a mature vulnerability program. Regular and thorough vulnerability scanning and monthly patching avoid the most preventable threats. Vulnerability scanning should cover the network perimeter, including the VPN or other remote access methods, as well as the internal network, since some attacks may bypass perimeter defenses. Once each scan is complete, address any detected vulnerabilities, starting with the most critical by severity and potential impact. Like painting a bridge, vulnerability scanning is a process that never really ends. A fully mature security posture includes a documented vulnerability management program that encompasses critical infrastructure protection.

IT Security Posture

In an immature security environment, those responsible for security don't know their security gaps, and even the most basic security assessment becomes a crucial step. As maturity develops, known security gaps become evident and remediated because the team follows up formal security assessments with the development and execution of a remediation roadmap.

Like painting a bridge, vulnerability scanning is a process that never really ends.

A proactive organization will find itself working on a full IT security framework, and it reaches best-in-class status when that framework is fully implemented and maintained.

Compliance

A security program also addresses compliance with the regulations and standards that affect an organization. It's essential to first understand which regulations, standards and certifications affect an organization: The most common compliance for U.S. organizations in regulated industries are HIPAA for healthcare and PCI DSS for the payment card industry. Outside of regulatory compliance, many organizations also adopt a best-practice standards framework to guide security and provide assurance to customers and partners. The most common of these security standard frameworks are NIST and ISO. A new initiative from the U.S. Department of Defense requires supply chain vendors to have Cybersecurity Maturity Model Certification (CMMC) to help safeguard the information within the U.S. defense supply chain.

As organizations become compliant and mature, they plan how to stay compliant as changes in their environments or compliance requirements occur. Specific security compliance activities may include a gap analysis, penetration testing and a detailed assessment report with remediation guidance. Third-party experts can perform these assessments to meet compliance requirements, provide an outside perspective and free the IT team to focus on what it does best.

Penetration Testing

Penetration testing—sometimes referred to as "ethical hacking"—is a similar bridge painting effort. The goal of a scheduled "pen test," which is best conducted by an outside third party, simulates a cyberattack and validates the efficacy of existing security controls. The pen test uncovers potential vulnerabilities in applications and the environment from incorrect hardware or software configurations, insufficient patching, changes in the environment or information discovered on the Dark Web. In a fully mature organization, penetration testing and follow-on remediation occur every quarter.

The second type of penetration testing is social engineering, which tests how well employees defend against cybercrimes. Well-trained employees are the first line of defense, especially since the most common bad actor entry point is phishing schemes. To optimize the front line of employee defense, train everyone across the organization, and perform follow-up social engineering testing. Regular and ongoing training and testing become critical for maximizing everyone's understanding of security policies and guidance. By educating and testing every employee, an organization has the best chance of protecting itself—train, test and repeat.

Privacy

Data privacy concerns are becoming increasingly important to customers. As a result, governments have created regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). A U.S. privacy law is likely in 2021 as three proposals are moving

THE TOP CYBERATTACK ACCESS VECTORS[13]

31%
Phishing

30%
Scan and exploit

29%
Unauthorized use of credentials

6%
Brute force attacks

2%
Mobile device compromise

1%
Watering hole attack

through Congress: the Consumer Data Privacy and Security Act (CDPSA), the United States Consumer Data Privacy Act and the Consumer Online Data Privacy Act (CODPA).

To meet data privacy requirements, the first rule is "if you don't need it; don't save it." Then determine which assets fall under the regulation, document where they reside and who may access them both inside and outside of the organization. Once the team understands all that, it's time to think about isolating and protecting that data and updating relevant policies and procedures to account for data privacy regulations. A fully mature organization performs ongoing updates to privacy-related policies and procedures and ensures compliance with applicable frameworks.

Incident Response

Current cybersecurity best practice acknowledges the likely inevitability of a security breach. To optimally manage that reality, IT teams need an up-to-date incident response plan. Mature organizations have well-documented incident response plans that specify process steps and are updated at least annually. Without a rapidly deployable plan, organizations scramble and take ad hoc measures when faced with a security breach. Delays and non-optimal actions can extend recovery time, cause more damage or lose valuable forensic data needed to understand what happened. Preserving and analyzing that forensic data is critical to building moats that prevent that type of breach from happening again. A well-prepared, well-trained team should act immediately to restore operations quickly and capture incident forensics. Incident response capability can be especially important in the case of a ransomware attack, when a clock is literally ticking.

Governance

Security governance documents codify the oversight policies and procedures for a security plan and ensure adherence to a security framework. No matter the size of the organization, it's vital to have policies clearly documented. The exercise of creating governing documents will automatically improve security maturity. Any organization that operates in a regulatory environment that demands tight security will have no choice but to take this step as passing audits require up-to-date policies and procedures.

The Five Levels of a Cybersecurity Maturity Journey

Advancing any organization's cybersecurity maturity is a journey. Flexential Professional Services built a cybersecurity maturity model to illuminate and navigate that journey. The model enables quick current-state identification and easy determination of the next actions and investments for strengthening cybersecurity defenses.

Each maturity level blends people, processes and technology aspects to yield actionable milestones. Use these nine elements and five levels, combined with understanding the organization's regulatory environment, customer requirements, risk appetite, budget and full hybrid IT environment to determine the current maturity level and a future-state target. Then use the maturity model to map a path for achieving that future state.

A U.S. privacy law is likely in 2021 as three proposals are moving through Congress: the Consumer Data Privacy and Security Act (CDPSA), the United States Consumer Data Privacy Act and the Consumer Online Data Privacy Act (CODPA)

Current cybersecurity best practice acknowledges the likely inevitability of a security breach.

Flexential Cybersecurity Maturity Model

There is no single correct answer for a future-state security posture; every organization has its own security needs, requirements and risk tolerance. The organization's hybrid IT footprint size and complexity, data sensitivity and data criticality also contribute to determining the plan. Understanding an organization's current maturity level and plotting a path forward requires careful thought and planning, but it's worth the effort. The costs of planning and executing on a maturity path will be dramatically less than the recovery costs of a debilitating security breach.

	Beginning	Developing	Advancing	Effective	Proactive
ROLES	No one dedicated to security	Responsible party for security	Dedicated security administrator	Growing a specialist security team	Full management and security team with certifications for cybersecurity, risk and compliance
RISK MANAGEMENT	No risk management	Annual risk assessment	Annual risk assessment	Annual risk assessment with risk register updated quarterly	Annual risk assessment with risk register continuously updated
VULNERABILITY MANAGEMENT	No vulnerability scanning and irregular vendor patching	Irregular vulnerability scanning and monthly vendor patching	Quarterly vulnerability scanning, monthly patching and remediation of critical vulnerabilities	Developing a best practice-based vulnerability management program	Vulnerability management program including proactive protection of critical infrastructure
IT SECURITY POSTURE	Does not understand security gaps	Knows biggest security gaps	Executed formal security assessment and developing a remediation roadmap	Working on implementing an IT security framework	Fully implemented IT security framework
COMPLIANCE	Not compliant	Understanding which compliance frameworks are required	Implementing changes to become fully compliant	Full compliance with all requirements	Full compliance and on track to meet future requirements
PENETRATION TESTING	No penetration testing	Uses vulnerability scanning in lieu of penetration testing	Annual penetration testing of infrastructure	Annual penetration testing of infrastructure and applications	Quarterly penetration testing of infrastructure, applications and social engineering
PRIVACY	Outdated or missing privacy policy documentation	Minimally documented privacy policies and procedures	Partially documented privacy policies and procedures	Fully documented privacy policies and procedures. Compliant with applicable frameworks	Ongoing updates to privacy policies and procedures. Compliant with applicable frameworks
INCIDENT RESPONSE	Ad hoc response to incidents	Ad hoc response to incidents	Creation of incident response plan	Fully documented incident response plan	Incident response plans updated annually
GOVERNANCE	Outdated or missing security policy documentation	Minimally documented and dated security policies and procedures	Mostly documented security policies and procedures	Fully documented security policies and procedures	Ongoing updates to policies and procedures

"Companies with advanced cybersecurity and privacy programs both prioritize customer experience more highly and report faster revenue growth than firms with lower maturity levels."[14]

Benchmark Your Cybersecurity and Privacy Maturity

Forrester Research
April 2020

Those who choose to stand still instead of advancing their cybersecurity maturity should evaluate the risks they'll be assuming with that decision. The fact is that 74% of organizations report having either ad hoc, inconsistently applied or non-existent security plans.[15] There is clearly much work to be done and large risks from a lack of action, as the latest supply chain breach has demonstrated to 18,000 organizations, including highly sensitive U.S. government agencies and departments. "It's not about whether your data will be stolen or destroyed," said Tom Kellermann, head cybersecurity strategist at VMware Carbon Black. "It's whether your entire brand, your digital persona and your transformation efforts will be used to attack your customers and your partners. There's no coming back from that."[16]

Don't cede the field to the adversary, and don't assume that bad actors will always be one step ahead. A recent Gartner analysis of clients' ransomware preparedness showed that over 90% of ransomware attacks are preventable.[17] Preparation will reduce the risk, losses and impacts when a security incident occurs.

Cybersecurity may be a constant and challenging battleground, but preparedness, diligence and persistence help the good guys tip the scales in their favor. **Wherever the bad guys choose to step across the organization's hybrid IT environment, get there one step sooner and build defenses to protect customers, data and operations.**

Partnering on the Path to Cybersecurity Maturity

No matter their current cybersecurity maturity level, organizations can benefit from engaging external experts to evaluate, guide, or manage a cybersecurity program—as well as remediate gaps or recover from ransomware incidents. Flexential cybersecurity experts have worked with thousands of customers and deal with cybersecurity defense, preparedness—and incidents—every day. Flexential Professional Services experts can guide a maturity journey to minimize cyber vulnerabilities and defend the confidentiality, integrity and availability of data.

Flexential Professional Services experts partner with organizations on cybersecurity, compliance, architecture and strategy, cloud migrations, cloud optimization, DevOps and IT resiliency to solve today's hybrid IT challenges. We take a consultative approach and tailor each engagement to customer needs. Our expertise, experience, and best-practice methodologies enable us to provide detailed, actionable guidance. Wherever data, applications, or infrastructure reside, Flexential Professional Services will partner with IT, security and risk teams to achieve the organization's transformation strategy and advance cybersecurity and compliance maturity.

A Gartner analysis of clients' ransomware preparedness showed that over 90% of ransomware attacks are preventable.[17]

1 https://newsroom.ibm.com/2020-06-30-IBM-Study-Security-Response-Planning-on-the-Rise-But-Containing-Attacks-Remains-an-Issue
2 https://notified.idtheftcenter.org/s/
3 https://www.ibm.com/security/data-breach
4 https://www.carbonblack.com/blog/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/
5 https://www.bitdefender.com/files/News/CaseStudies/study/348/Bitdefender-10-IN-10-The-Indelible-Impact-of-COVID-19-on-Cybersecurity.pdf
6 https://newsroom.ibm.com/2020-06-22-IBM-Security-Study-Finds-Employees-New-to-Working-from-Home-Pose-Security-Risk
7 https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
8 https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report
9 https://apnews.com/article/technology-hacking-u-s-news-business-d4e46b99d0613bb9c967b868bd751a46
10 https://www.aon.com/unitedkingdom/insights/reputational-damage-and-cyber-risk.jsp
11 https://www.ibm.com/security/data-breach/threat-intelligence
12 https://cpl.thalesgroup.com/data-threat-report
13 IBM X-Force Threat Intelligence Index 2020, https://www.ibm.com/account/reg/us-en/signup?formid=urx-42703
14 Benchmark Your Cybersecurity And Privacy Maturity, 2020. The Benchmark Report In The Cybersecurity And Privacy Playbook by Merritt Maxim and Elsa Pikulik April 28, 2020
15 https://www.cybersecasia.net/news/more-security-tools-in-use-do-not-equate-to-better-security-study
16 https://www.sdxcentral.com/articles/news/vmware-what-to-do-when-cybercriminals-hunt-your-company-in-your-home/2020/04/
17 https://www.gartner.com/en/documents/3978727/defend-against-and-respond-to-ransomware-attacks

ABOUT FLEXENTIAL

Flexential empowers the IT journey of the nation's most complex businesses by offering flexible and tailored hybrid IT solutions comprised of colocation, cloud, connectivity, data protection, managed, and professional services. The company builds on a platform of three million square feet of data center space in 20 highly connected markets, and on the FlexAnywhereTM 100GB private backbone to meet the most stringent challenges in security, compliance, and resiliency. See how Flexential goes beyond the four walls of the data center to empower IT through an interactive map found on www.flexential.com.