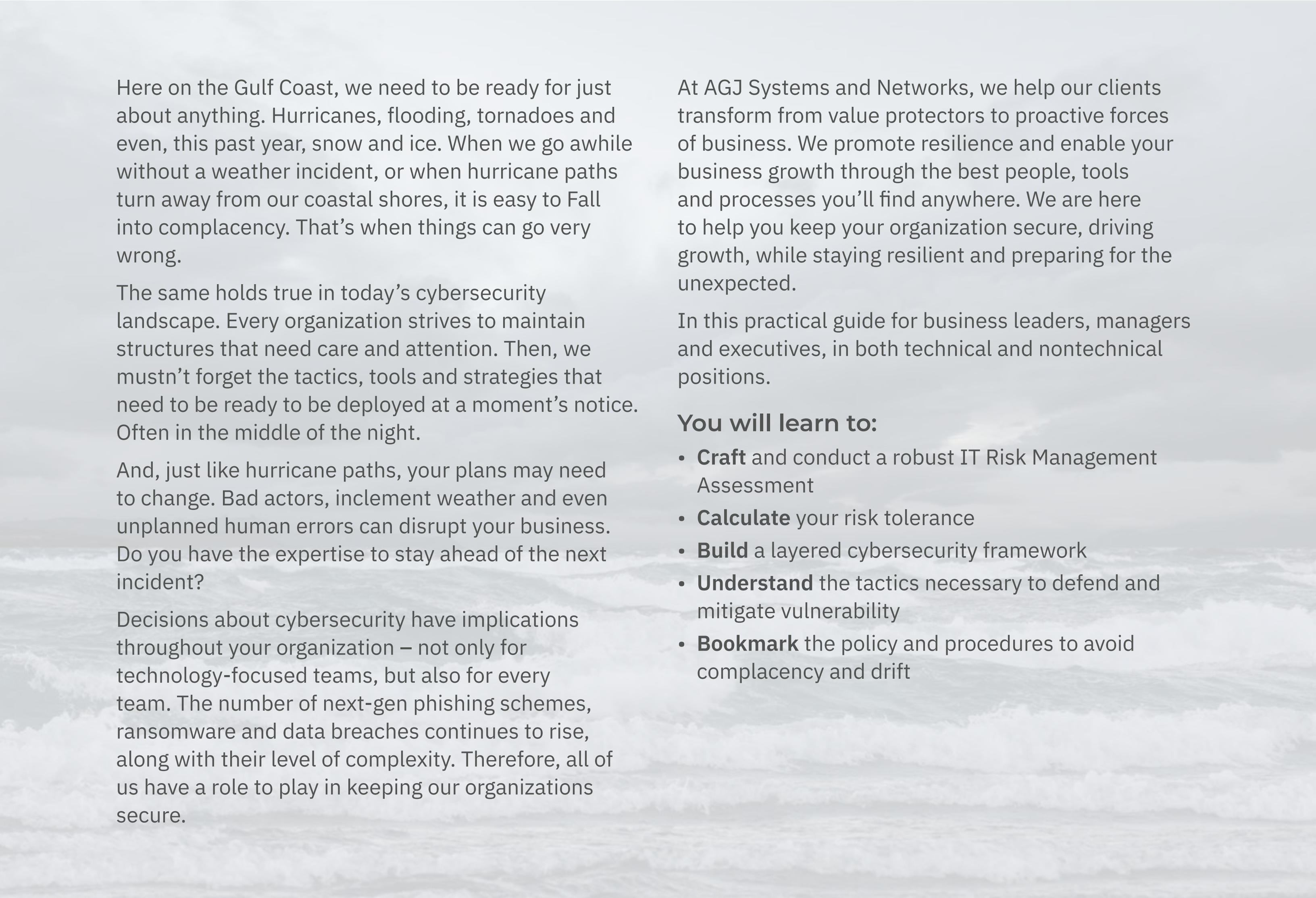
A Gulf Coast Cybersecurity Playbook

Why your IT preservation strategy should resemble hurricane preparations

agj

your IT department

20 years



Here on the Gulf Coast, we need to be ready for just about anything. Hurricanes, flooding, tornadoes and even, this past year, snow and ice. When we go awhile without a weather incident, or when hurricane paths turn away from our coastal shores, it is easy to Fall into complacency. That's when things can go very wrong.

The same holds true in today's cybersecurity landscape. Every organization strives to maintain structures that need care and attention. Then, we mustn't forget the tactics, tools and strategies that need to be ready to be deployed at a moment's notice. Often in the middle of the night.

And, just like hurricane paths, your plans may need to change. Bad actors, inclement weather and even unplanned human errors can disrupt your business. Do you have the expertise to stay ahead of the next incident?

Decisions about cybersecurity have implications throughout your organization – not only for technology-focused teams, but also for every team. The number of next-gen phishing schemes, ransomware and data breaches continues to rise, along with their level of complexity. Therefore, all of us have a role to play in keeping our organizations secure.

At AGJ Systems and Networks, we help our clients transform from value protectors to proactive forces of business. We promote resilience and enable your business growth through the best people, tools and processes you'll find anywhere. We are here to help you keep your organization secure, driving growth, while staying resilient and preparing for the unexpected.

In this practical guide for business leaders, managers and executives, in both technical and nontechnical positions.

You will learn to:

- **Craft** and conduct a robust IT Risk Management Assessment
- **Calculate** your risk tolerance
- **Build** a layered cybersecurity framework
- **Understand** the tactics necessary to defend and mitigate vulnerability
- **Bookmark** the policy and procedures to avoid complacency and drift

2020 was a year of records, both on the ground and in cyberspace.

Weather records (Gulf Coast)

- **26** tornadoes
- **12** Named storms
- Rainfall: **8 inches** above normal

Cyber (worldwide)

- Data breaches exposed **36 billion records** in the first half of 2020. (Risk Based)
- The average ransomware payment **rose 33%** in 2020 over 2019, to $111,605. (Fintech News)
- After declining in 2019, phishing **increased in 2020** to account for 1 in every 4,200 emails. (Symantec)

You must understand your risks before you can address them

Just as with predicting landfall for hurricanes, with threats to sensitive data growing in both number and sophistication every day, organizations cannot afford a spaghetti hurricane model approach to security. Instead, you need to focus your limited IT budget and resources on the specific vulnerabilities in your unique security posture.

To do this, treat vulnerabilities as a piece of a larger satellite map, influenced by a variety of internal and external factors. You need to identify, analyze and prioritize the risks to the confidentiality, integrity or availability of your data or information systems, based on both the likelihood of the event and the level of impact it would have on the business. This process is called IT risk assessment and should be completed every year, preferably by an unbiased IT expert like AGJ.

IT Risk Assessment Steps

1. Identify and Prioritize Tech Assets

Any equipment or software that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information, including:

- Printers
- Storage devices
- Computers
- Computer equipment
- Network equipment and systems (routers, switches, application delivery controllers and the vendor tools that manage them)
- Security controls, such as firewalls, secure web gateways (SWG) and cloud security tags, intrusion prevention systems (IPSs), virtual private networks (VPNs) and a vector directory number (VdN)
- Public and private cloud services, such as Amazon Web Services, Microsoft Azure, Cisco ACI and VMware NSX, as well as their provided management tools
- Asset repositories, including endpoint security systems (EDRs), patch management systems, configuration management databases (CMDBs) and homegrown databases
- Vulnerability occurrence data from vulnerability scanners, web and app scanners, asset configuration weaknesses and custom vulnerabilities
- Phone equipment and systems

HOW TO

Define a standard for determining the importance of each asset.

Common criteria include:

- Role/importance to organization
- Monetary value
- Age
- Location
- Exploitability
- Legal standing (compliance)

Classify each asset as critical, major or minor.

2. Understand Threats

- Natural disasters
- Hardware and software failures
- Accidental employee error

Malicious behaviors, such as:

- Interference (deleting data, distributed denial of service (DDOS) or stealing equipment
- Interception – theft of your data
- Impersonation – misuse of someone else's credentials, via social engineering attacks, brute-force attacks or Dark Web purchase

HOW TO

- Ongoing cybersecurity awareness training events
- Onsite/offsite backup disaster recovery plan
- Deploy a layered approach to security
- Enable MFA

3. Pinpoint Vulnerabilities

- Consider the likelihood that vulnerability will be exploited and a threat will succeed against an organization's defenses.

Broad categories of these vulnerability types include:

- Network Vulnerabilities — Issues with a network's hardware or software that expose it to possible intrusion by an outside party such as WiFi access points and poorly configured firewalls
- Operating System Vulnerabilities occur within a particular operating system that hackers may exploit to gain access to an asset the OS is installed on – or to cause damage. Examples include a super user account that may exist in some OS installs and hidden backdoor programs. Poor Patching Hygiene, IE: Not patching on a regular basis, allowing for vulnerability.
- Human Vulnerabilities — Accidentally expose sensitive data, create exploitable access points for attackers or disrupt systems
- Process Vulnerabilities — Created by improper or missing process controls, such as use of weak passwords

HOW TO

Vulnerabilities can be identified through:

- Business impact analysis (BIA) or mission impact analysis report.
- Third-party analysis
- Audit reports
- The NIST vulnerability database, vendor data
- Information security test
- Evaluation (ST&E) procedures
- Penetration testing
- Automated vulnerability scanning tools

For each, determine:

- Where the vulnerability exists
- What caused it
- How it could be used

4. Classify and Analyze Controls

Two broad categories of controls include:

Technical controls

- Encryption
- Intrusion detection and prevention mechanisms
- Identification and authentication solutions
- MFA

Nontechnical controls

- Security policies
- Administrative action
- Physical and environmental mechanisms

Another way could be ...

- Inventory of Un/Authorized Devices
- Inventory of Un/Authorized Software
- Secure Configurations for Hardware/Software
- Continuous Vulnerability scanning and remediation
- Controlled Use of Administrative Privileges

Can further be classified as:

- Preventive: Controls attempt to anticipate and stop attacks; examples include encryption and authentication devices
- Detective: Controls are used to discover threats that have occurred or are in process; they include audit trails and intrusion detection systems

HOW TO

Monitor and minimize or eliminate the probability that a threat will exploit vulnerability.

Deploy Multifactor Authentication (MFA)

Following framework – mapping tools into controls

User awareness training - analyze and understand how an attack affects you.

5. Determine Likelihood of Incident

Assess the probability that a vulnerability might actually be exploited, taking into account the type of vulnerability, the capability and motivation of the threat source and the existence and effectiveness of your controls.

Analyze the impact that an incident would have on the asset that is lost or damaged, including the following factors:

- The mission of the asset and any processes that depend upon it
- The value of the asset to the organization
- The sensitivity of the asset

Use the categories high, medium and low to assess the likelihood of an attack or other adverse event.

HOW TO

To get this information, start with a business impact analysis (BIA) or mission impact analysis report. This document uses either quantitative or qualitative means to determine the impact of harm to the organization's information assets, such as loss of confidentiality, integrity and availability. The impact on the system can be qualitatively assessed as high, medium or low.

6. Prioritize the Information Security Risks

For each threat/vulnerability pair, determine the level of risk to the IT system, based on the following:

- The likelihood that the threat will exploit the vulnerability
- The approximate cost of each of these occurrences
- The adequacy of the existing or planned information system security controls for eliminating or reducing the risk

Using the risk level as a basis, determine the actions needed to mitigate the risk. Here are some general guidelines for each level of risk:

- High – Corrective measures should be implemented as soon as possible
- Medium – A plan should be developed within a reasonable period of time
- Low –The IT team must decide whether to accept the risk or implement corrective actions

HOW TO

As you evaluate controls to mitigate each risk, be sure to consider:

- Organizational policies
- Cost-benefit analysis
- Operational impact
- Feasibility
- Applicable regulations
- The overall effectiveness of the recommended controls
- Safety and reliability

7. Document Results

Based on all the above documentation, develop a risk assessment report to support management in making appropriate decisions on budget, policies, procedures and talent allocations.

The risk assessment report can identify key remediation steps that will reduce multiple risks.

Each step should detail the associated cost and the business reasons for making the investment.

HOW TO

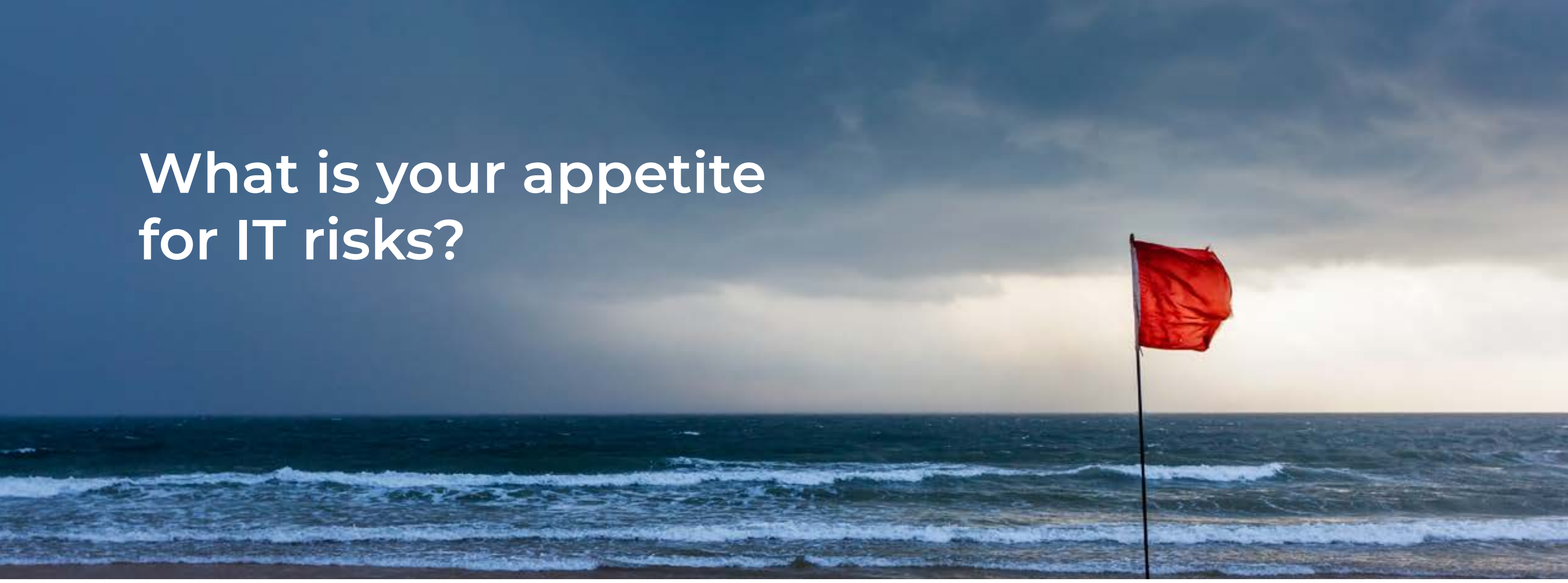
Understand your risk by:

- Determining costs associated with risk
- Prioritizing resource allocations based on your risk assessments
- Working with qualified professionals to verify that your report is properly written.

As you work through this process, you will get a better idea of how your organization and its infrastructure operate. From there your organization can develop an IT risk assessment policy that defines:

- What the organization must do annually
- How risk is to be addressed and mitigated
- How the organization must carry out future risk assessments

What is your appetite for IT risks?



Now that you have identified the vulnerabilities and threats that could disrupt your day-to-day business operations, it's time to address your organization's willingness to take on certain risks.

Big or small, regulated or not, all organizations must assume some degree of IT risk. Most proactively seek to reduce risk and minimize its potential impact through a comprehensive risk management policy. While some risks are necessary and can drive positive business outcomes, others can lead to negative impacts, such as operating errors, poor strategic decision making, accidents, potential legal exposure or financial uncertainty. Organizations must accept that not all risks are avoidable, but they do have control over the scale and scope of risks they are willing to take.

Appetite + Tolerance = Posture

Risk appetite: No, this is not a spicy Cajun menu evaluation. This concept refers to a target level of loss exposure that the organization views as acceptable, given business objectives and resources. To effectively deploy a risk appetite framework, an organization must adopt an agreed risk measurement and risk-scoring methodology, as well as a common risk language, in order to be consistently understood and applied throughout your organization.

Risk tolerance: Risk tolerance defines the boundaries within which your organization is comfortable operating, given its overall risk appetite. It determines the degree of variance from the organization's risk appetite that the organization is willing to tolerate.

Factors and metrics to help you decide your path include:

How much risk?

- Financial/Credit
- Operational
- Third-party
- Information security
- Compliance
- Legal risks
- Brand trust

Defining metrics

- Acceptable loss
- Credit ratings
- KPI limits
- Probabilistic measures
- Qualitative measures
- Balance sheet metrics.

Key to your cyber posture is determining your RPO and RTO.

Recovery Point Objective (RPO) indicates the amount of data (updated or created) that will be lost or need to be re-entered after an outage. RPO answers the question: If a disaster occurs between backups, can you afford to lose 10 minutes' worth of data updates? Or 10 hours? How about a full day? More?

Recovery Time Objective (RTO) represents the duration of time between loss and recovery and the steps IT must take to restore the application and its data. In a high-frequency transaction environment, seconds of being offline can represent thousands of dollars in lost revenue, while other systems could go dark for hours without a significant adverse impact to your business. RTO answers the question: How long can it take for our system to recover after we are notified of a business disruption?

Your cyber risk posture

Not all data is equally critical to business operations. The shorter the downtime, the more costs and processes it takes to meet those benchmarks. From the above exercise, you can better manage the balancing act needed to determine which systems and types of data are worth larger investments to achieve those short RTOs and RPOs.

The building blocks to a superior cyber posture

A layered approach to defend against bad actors

The biggest threat to your organization is thinking you don’t need cybersecurity. You may believe that your organization isn’t big enough or that your information isn’t valuable enough to be enticing. However, hackers aren’t choosy: (https://www.scmagazine.com/home/security-news/ransomware/ransomware-attack-cost-new-orleans-7-million-and-counting/)

They are constantly finding new ways to obtain sensitive data, so it’s critical to stay on top of changes in your unique IT landscape and manage your risk profile.

Common Types of Attack

According to Security Boulevard, 2020 saw global losses of more than $3.5 billion, just to email compromise. Just last year, a ransomware attack on New Orleans has racked up at least $7 million in financial damage.

Cyberthreats are a serious problem. We have summarized the worst of the worst below:

THREAT TYPE	ORIGIN	MITIGATION
Ransomware A type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid	Most often coming from email, but also as a result of insecure protocols, drive-by downloads, USB and removable media and event social media	Train your staff to: A) Recognize potential sources, such as • Applications or attachments in emails requesting permissions not normally required • Duplicate files of the same name and type with different extension endings B) Identify when their system has been compromised, and stop it from spreading further into the organization. Utilize Security Tools uniquely designed to contain the spread of these risks.
Dedicated Denial of Service (DDOS) Legitimate users are unable to access information systems, devices or other network resources due to the actions of a malicious cyberthreat actor.	Most often accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes.	Deploy a security operations center (SOC) within your network operations center to provide: • A centralized point of function to monitor and track incidents and threats • A proactive approach to identify a threat early on • Partner with an expert MSP to handle these important functions for you:

Social engineering **Phishing** **Keyspoofing** A cyberattacker pretends to be from your organization	**3 methods:** • **Email** – a sender fakes an email address. • **IP Spoofing** – an attacker hides their computer or network address or fakes yours • **Online usernames** for social media, discussion boards or other public forums, where an attacker pretends to be you	• Hover over links and check the URL before you click • Don't open email attachments you weren't expecting • Consider flagging external emails • Be cautious in responding to emails or online requests, especially with sensitive information • Use robust passwords that you change frequently • Monitor your online presence
Zero-Day Attackers release malware before a developer has an opportunity to create a patch to fix a vulnerability	The attacker writes and implements exploit code, while the vulnerability is still open and available. After releasing the exploit, either the public recognizes it in the form of identity or information theft, or the developer catches it and creates a patch to staunch the cyber-bleeding. Use artificial intelligence and machine learning to look for patterns	• Use artificial intelligence and machine learning to look for patterns • Utilize tools that flag suspicious activity • Follow up on suspicious activity and reference against past incidents • Issue patches
Keylogging **Malicious Bots** **Virus and Trojans**	Malicious software programs installed into the victim's system, sending data back to the hacker. They can also lock your files, serve fraud advertisements, divert traffic, sniff your data or spread on all the computers connected to your network.	Ensure you have next generation antivirus and Endpoint Detection and Response (EDR) tools
Man-in-the-Middle Attack **Cookie Theft** (aka SideJacking or Session Hijacking) **DNS poisoning** Gaining access to a personal data such as browsing history, username and passwords for different sites we access, a hacker can authenticate himself as you on a browser.	A hacker manipulates a user's IP packets to pass through to an attacker's device.	• See guidance for Zero Day • Deploy user awareness training
Click Jacking Attacks UI (aka Redress)	A hacker hides the actual UI where the victim is supposed to click. This behavior is very common in app download, movie streaming and torrent websites and can be used to steal your personal information.	• Deploy user awareness training • Ensure you have next generation antivirus and Endpoint Detection and Response (EDR) tools

Tactics and Layers

Ransomware, phishing scams and malicious email attachments, hacker attacks – the list of potential cybersecurity threats just continues to grow. Most experts agree that it's a matter of when, not if, an organization will be the target of a cyberattack.

In an age when no two network threats are exactly alike, it is important to understand that different cybersecurity threats call for different security measures. But simply adding an array of security tools isn't enough. As we noted earlier, a fragmented approach to security can make it harder to identify and respond to threats.

The best defense is a layered security architecture that recognizes both the strengths and limitations of various security products. Also known as defense in depth, layered security places multiple security controls throughout the IT environment. If an attack bypasses one security tool, others can be deployed to increase the odds that an attack will be identified and stopped.

SIEM (Security information and event management) And Security operations center (SOC)

- Intrusion prevention and detection
- IT service management
- Identify access manager

Perimeter Security and Network Security

- Next generation firewall
- Site-to-site connections
- Web content filtering
- Remote services
- VPN service

Endpoint Security

- MFA
- Endpoint detection and response
- Patch management (hard to keep up with this)
- Anti-virus
- Managed detection and response (MDR)
- Device hardening

Application Security

- Application whitelisting and blacklisting
- Third party application patch management

Data Security

- Data encryption (at rest and in transit)
- Data classification
- Data loss prevention and auditing (refer to SIEM)
- Vulnerability/Pen test Scanning

Policy Management

- Access control
- Data protection
- Encryption
- Remote access
- Zero trust
- Least access
- Third-party assessments
- Risk assessments
- Training
- RPO-RTO
- Backup and disaster recovery
- Dark Web scan

Focus on Training

Support your enhanced cybersecurity efforts with training, both for your IT staff and for general workers.

Since attacks can enter your organization through a variety of doors, and a lot of compromises begin based on user actions, making cybersecurity everyone's job increases program effectiveness.

We recommend requiring this initial training for all current staff and as part of the onboarding process for new staff. In addition, we recommend regular refresher training and ongoing email drills to keep cybersecurity at the front of everyone's minds.

Consider also creating all-hands staff training for the following:

- Email security, such as recognizing phishing attempts and other email malware
- Internet behavior, such as recognizing suspicious links and dangerous websites
- Computer desktop security, such as locking Windows desktops before walking away from desks, and any password storage guidelines your organization requires

What does effective user-awareness training look like? Elements include:

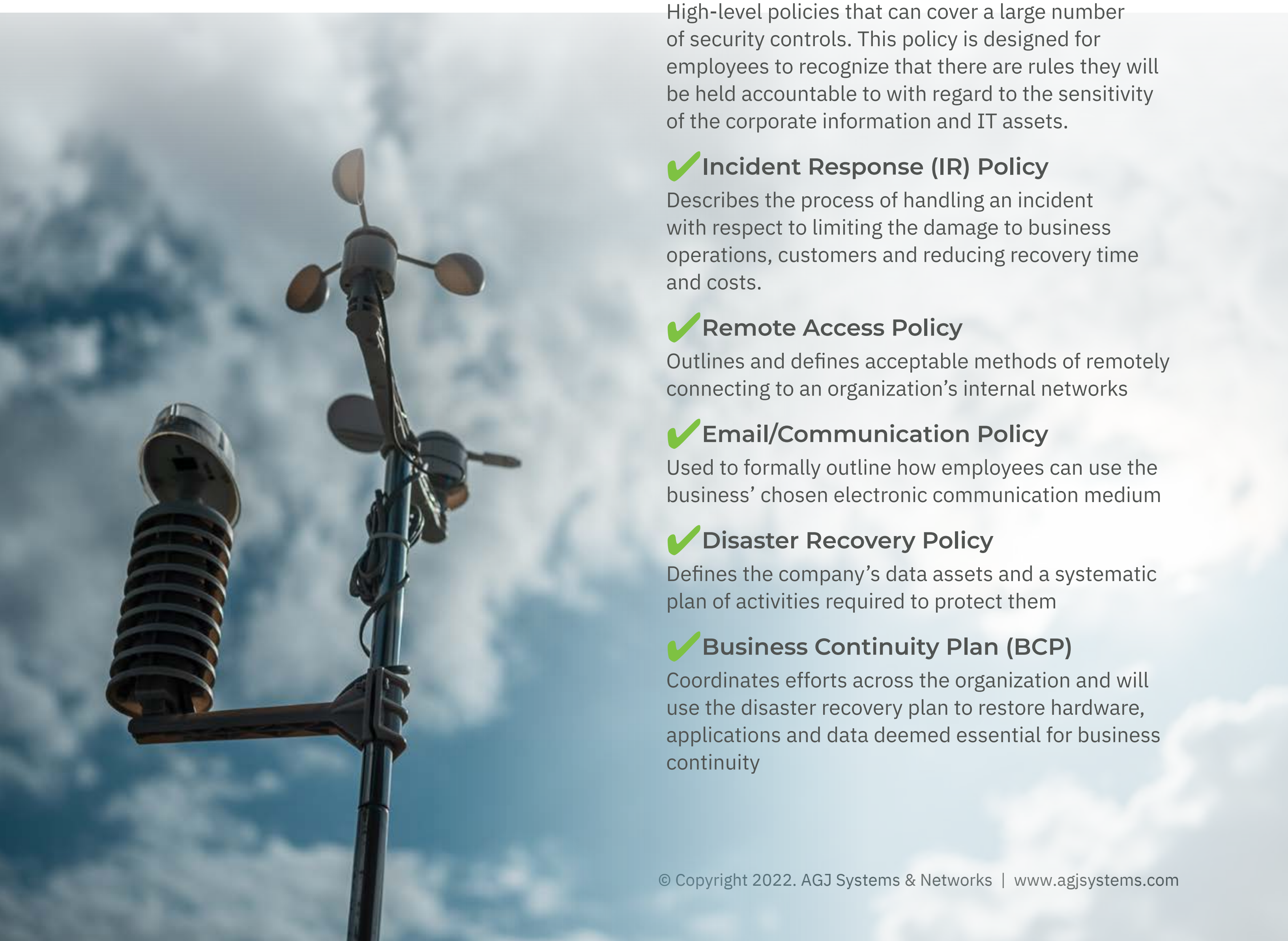
- Regular mandatory employee training
- Scheduled awareness surveys
- Unscheduled awareness assessments to measure compliance with user-awareness training
- Feedback surveys designed to improve ongoing training programs

Policy & Procedures Essentials

Even with a cybersercurity program in place, your policy and procedures are more important than the tools to protect your business.

The key to a successful cybersecurity plan is to ensure your documentation matures and grows as your organization does. Many organizations create cybersecurity policies and procedures, then put them on a shelf and call it a job well done. Because cyberattackers are always evolving, your cybersecurity plans need to as well.

Develop or enhance your organization's cybersecurity policies and procedures to ensure they align with supported best practices and match the baseline risk tolerance you have now established. Consider including a defined policy for how and when to update the policies and procedures as you add and remove devices or enhance your baseline.



✓Acceptable Use Policy (AUP)

Stipulates the constraints and practices that an employee using organizational IT assets must agree to in order to access the corporate network or the internet. It should be standard onboarding policy for new employees.

✓Access Control Policy (ACP)

Outlines the access available to employees in regard to an organization's data and information system

✓Change Management Policy

Refers to a formal process for making changes to IT, software development and security services/ operations. The goal is to ensure that all changes are conducted methodically to minimize any adverse impact on services and customers.

✓Information Security Policy

High-level policies that can cover a large number of security controls. This policy is designed for employees to recognize that there are rules they will be held accountable to with regard to the sensitivity of the corporate information and IT assets.

✓Incident Response (IR) Policy

Describes the process of handling an incident with respect to limiting the damage to business operations, customers and reducing recovery time and costs.

✓Remote Access Policy

Outlines and defines acceptable methods of remotely connecting to an organization's internal networks

✓Email/Communication Policy

Used to formally outline how employees can use the business' chosen electronic communication medium

✓Disaster Recovery Policy

Defines the company's data assets and a systematic plan of activities required to protect them

✓Business Continuity Plan (BCP)

Coordinates efforts across the organization and will use the disaster recovery plan to restore hardware, applications and data deemed essential for business continuity

Now What?

Gap Analysis

Contract with a security-first managed services provider (MSP) like AGJ to examine your current infrastructure, compliance requirements and existing cyber posture to identify and prioritize areas of improvement.

Ongoing Auditing

Regularly performing security audits is the best way to assess what security measures should be employed in protecting your connected assets and when to implement those fixes. Security audits capture all the pertinent information regarding security for each device.

Identify the current state of your organization's cybersecurity program (where you are), then determine what needs to be enhanced to reach an optimal baseline. Finally, develop an action plan for implementing improvements to reach that baseline.

Reporting

Oversight is also about accountability, ensuring remediation plans are carried out effectively and accurately. To understand if vulnerability is truly eliminated from your network, the oversight phase should include discovery processes, beginning the entire vulnerability management process again for any unaddressed occurrences.

Monitoring

Check for changes in network exposure and exploit activity, escalating vulnerabilities to imminent threats when necessary.

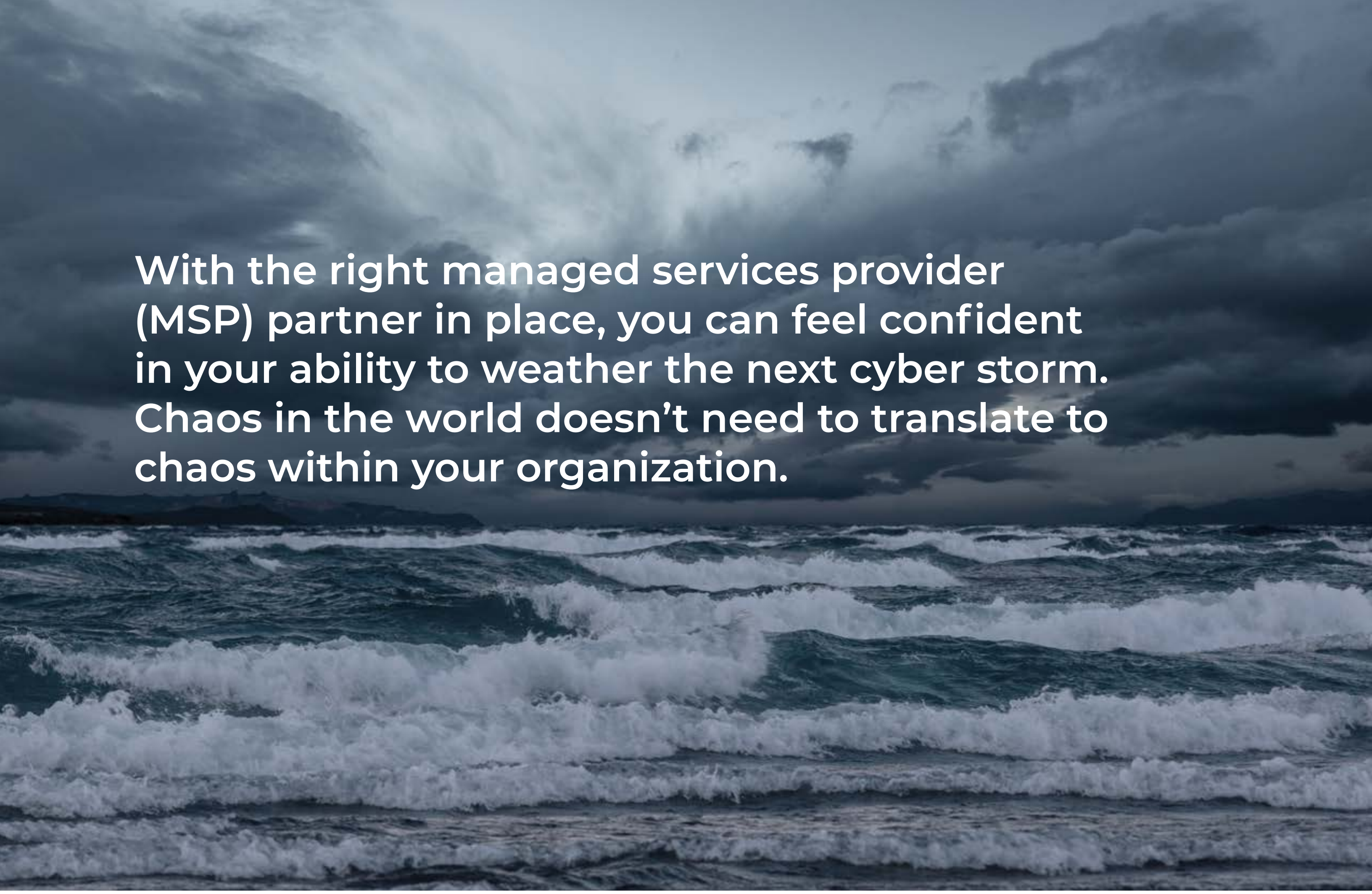
Creating a cyber culture with buy-in from leadership

Prevention is cheaper than remediation. Most calls to AGJ for advanced cybersecurity protection are a result of an incident or due to forced regulation.

C-Suite executives are busy, keeping track of profits and many people and projects at once. Nevertheless, this can't be an excuse for not keeping up with cybersecurity. Despite so many high-profile and catastrophic cybercrimes having been reported in the media, many leaders still have blinders on when it comes to the importance of proper cyber protection.

Consider the financial risk that is at stake with noncompliance. According to the Ponemon Institute's Cost of a Data Breach Report, in 2020, data breaches on average cost $3.86 million.

Employees represent one of the biggest threats to IT's efforts to protect applications, networks, systems and physical premises. Therefore, a commitment to cybersecurity needs to be followed by all members of the organization, including those at the very top.



With the right managed services provider (MSP) partner in place, you can feel confident in your ability to weather the next cyber storm. Chaos in the world doesn't need to translate to chaos within your organization.

As the go-to IT management provider for the Gulf Coast area, AGJ's team of veteran engineers knows everything there is to know about network security solutions and implementing the latest technologies.

AGJ provides the industry's broadest cybersecurity management solutions to address security challenges within large, complex networks.

Our LeapSecure® Security Suite provides comprehensive attack surface visibility and the context needed for informed action. Our analytics, automation and intelligence improve the efficiency and performance of security operations in vulnerability and threat management and firewall and security policy management for the world's largest organizations.

All modules of the LeapSecure® Security Suite work together and share information to ensure all recommended actions are consistent with compliance requirements and take into account the context of your organization's risk posture.

We help your organization:

- Proactively identify issues most likely to be exploited in an attack and continuously monitor for policy violations
- Prioritize vulnerabilities and security weaknesses in context to target action where it's needed most
- Intelligently plan response to systematically reduce your organization's risk of cyberattack and meet compliance requirements
- Centrally manage security data from hybrid network environments, security controls, assets and vulnerabilities

14257 Dedeaux Rd
Gulfport, MS 39503
United States

Phone: 228-300-9542

www.agysystems.com

agj
your IT department

| www.agjsystems.com