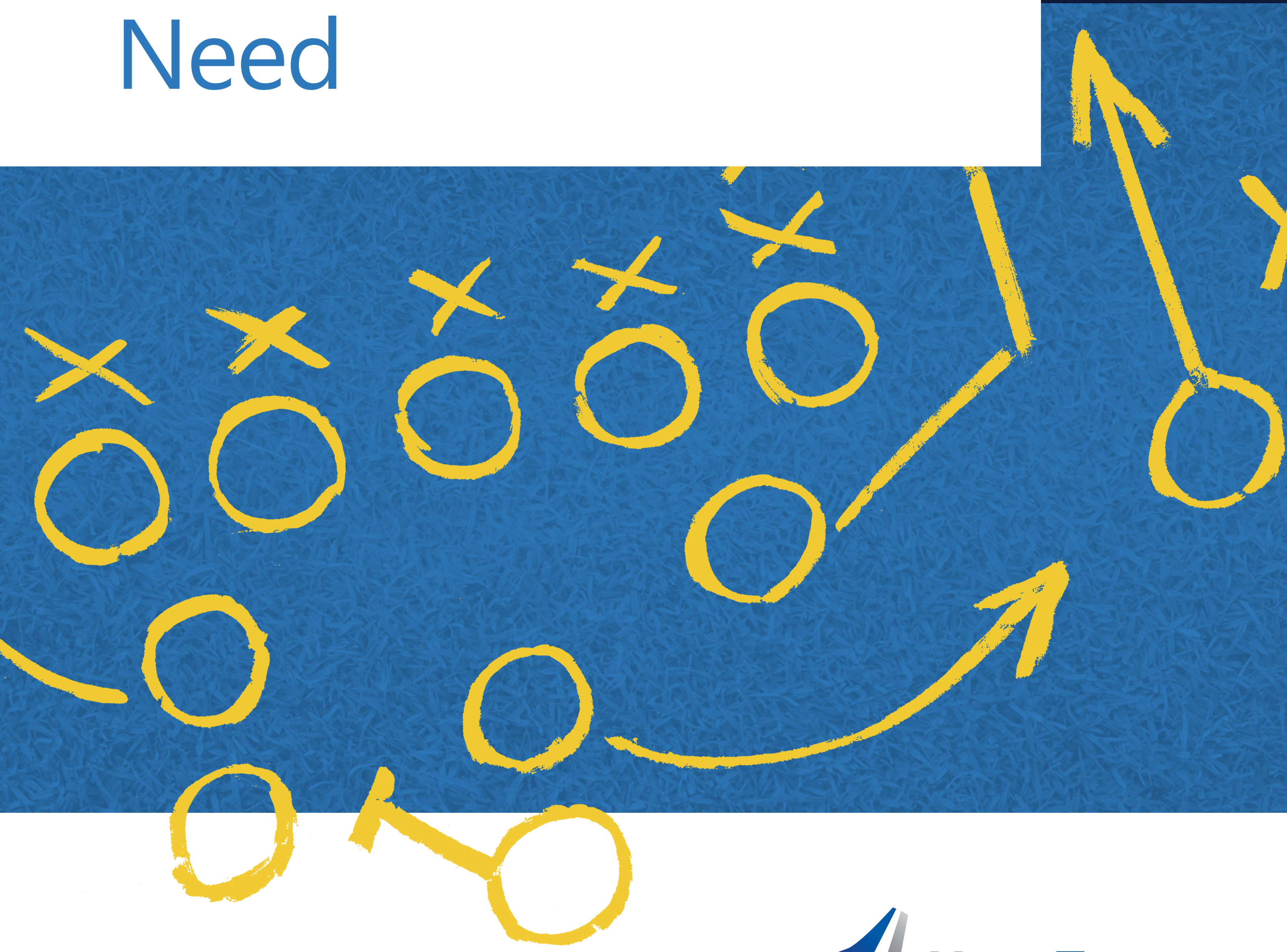
The IT Security Playbook All Organizations Need



VersaTrust

The Stakes of this Game Couldn’t Be Higher

As a business owner you’re the Head Coach of a team of star players. You work together to deliver value to your clients, fend off competitors and grow your business. Far from a friendly scrimmage, the stakes are high and the opposition is fierce.

Few opponents can strike as fast or immobilize you as completely as a Cyberattack. Every Head Coach needs a Defensive Coordinator and often it’s best to bring in that expertise from outside the organization.

That’s where we come in and this is our **Compliance and IT Security Playbook**.

The Ground Rules

Cybersecurity is not a one-time purchase. Even your top-shelf antivirus quickly becomes obsolete without routine monitoring, maintenance and upgrades.

You store sensitive information about your clients, employees and partners. If the data is stolen, their identities and your reputation are on the line. Or, cybercriminals can lock you out of your own systems, stopping work entirely. To remain a trusted, well-regarded organization, it’s essential to budget for IT. It doesn’t have to be expensive, but it does require a line item.

Keys to a Powerhouse IT Defense

5 Control Areas You Need to Defend

Establishing a strong defense is complicated. To help, we've broken down the various plays into 5 control areas:

1

Tackle Vulnerabilities with Cybersecurity Policies

To protect your organization, you must tackle all the IT risks you face. Before you can do this, you need to identify your weaknesses. Start with a risk assessment. The risk assessment identifies the universe of potential and likely threats that your institution faces. You can use this to build your Information Security Plan (ISP).

Risk Assessment > Information Security Plan > Cybersecurity Policies

The ISP details the measures you will take to prevent or counter the perceived threats and is the foundation for the cybersecurity policies you create.

Definition: Cybersecurity Policies

Cybersecurity policies establish the rules, procedures and responsibilities that will govern your approach to IT security.

Some examples of cybersecurity policies include:

- Prohibition on staff accessing bit torrent sites.
- Requirement that staff receives semiannual security training.
- Permission level granted to specific individuals based on their role and responsibilities.

2

Add Fumble-proof Data Backups to Your IT Security Roster

An effective backup protocol relies on two essential elements. Frequent and routine implementation is obvious. Less obvious is the type, quality and location of the storage medium.

For example, some organizations backup their data on aging tape cartridges. Tapes often exceed their lifespan of 250 passes long before their expiration date.

Moreover, onsite backup of an on-premise network introduces a particularly acute vulnerability to theft and natural disaster. A fire or flood that destroys your network (necessitating the need for backups) will almost certainly spoil your backups as well. In short: tape backups are more cumbersome and less reliable than more contemporary, off-site solutions.

3

Don't Let Your Business Get Sacked

No fan wants to see the opposing team break through their offensive line and sack their quarterback. Think of patching and software upgrades as the O-line for your business.

Often, these patches repair enormous security vulnerabilities. You may not be aware of these vulnerabilities; it's hardly in anyone's best interest to advertise them as it can alert hackers to exploit them (and you). Instead, most software companies will run patches regularly to quietly repair these gaps.

Without regular patches to all your software, you can assume your business is at risk of being sacked. Regularly patch and upgrade your systems.

4

Practice Makes Perfect: Ongoing Training for Your Team

Your team will continue to accidentally click links sent by hackers until they understand the threat. Expecting your employees to instinctively know what to do is like relying on raw talent to win the Super Bowl. You may fare well for a while but, in the end, the better prepared team will triumph.

Some of the costliest breaches happen from an employee clicking on a phishing email. Cybersecurity awareness training gives your team critical practice so they know exactly what to do when they receive phishing campaigns.

But only requiring the course would be like a football team skipping drills – without extra practice, they're more likely to make a mistake in the game. Cyberthreats are constantly evolving. Through tools like phishing security and reply tests, we'll help you drill the right defensive moves. When at actual attack appears, your team will automatically know what to do. We can help train people who fall outside the regulation too – like contractors or temps. Many of these support personnel interact directly with the network or through peripheral devices like WiFi routers and printers. Many also bring their own devices which are a gateway for hackers.

5

Block That Virus! Why Technical Configuration Matters

Technical configuration practices include the measures you take to establish a secure firewall, passive and active antivirus scanning, and encrypted VPNs. These measures also include user access, passwords and permission levels.

Take permission levels as one important example. Each staff member – or intern or consultant, for that matter – should be granted the lowest level of network access that they need to perform their daily duties. For non-daily activities, such as installing a new program or accessing a separate printer, admin authorization should be required.

Establishing secure configurations for your network and the software that protects it are increasingly essential as workplaces allow Bring-Your-Own-Device opportunities for employees and where outside consultants and other visitors log into the system to access the WiFi and access files.

It Takes a Team to Win

There's no single star player when it comes to cybersecurity defense. Like having a good cornerback without a strong defensive tackle, the various security tools like firewalls, antivirus and two-factor authentication work best when deployed as part of an integrated, multilayered defense.

It is critical to achieve a balance between safety and the efficient flow of business. Striking that difficult balance requires expertise and an intimate knowledge of your processes.

Engaging a trusted IT partner is the best and most efficient way to leverage the cybersecurity expertise you need. At VersaTrust, we get to know your operations so we can develop an effective, layered security infrastructure that works with your budget and your workflow.

Businesses throughout Fort Worth rely on VersaTrust to support and secure their organizations. We can help you tackle cybercriminals too. Contact us by phone (817-595-0111) or email today to get started.

We regularly partner with cities and businesses to support their IT needs and keep them safe.

Contact us by phone (817-595-0111) or email today.

VersaTrust