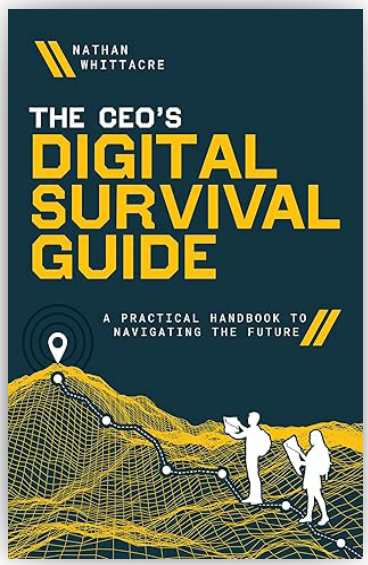
The CEO's Digital Survival Guide

A Practical Handbook to Navigating the Future

Nathan Whittacre



ISBN: 978-1-64225-630-7
Estimated reading time of summary: 7 minutes

Key Takeaways

- To operate securely, train your employees to protect the company from hackers and malware.
- Maintain your company's hardware by purchasing warranties, conducting regular check-ups, and learning when each piece will need to be replaced.
- An effective cybersecurity plan comprises a diverse collection of protective software and safeguard strategies.
- Protect your company against technological failures by providing backup power supplies, redundant Internet connections, and business continuity systems.

Overview

To be competitive in today's markets, companies must implement the right computer and data communication networks. However, few leaders understand how to select and maintain these technologies. In **The CEO's Digital Survival Guide**, information technology (IT) professional Nathan Whittacre explains how to overcome this common knowledge gap to build an effective, top-down digital strategy that improves your company's productivity and cybersecurity.

A Digital Self-Assessment

To develop effective technology systems, you must first assess your company's current digital state. This requires you to determine how it's doing in the following categories:

- *Infrastructure*. Does your company maintain a detailed inventory of all its workstations, servers, and network equipment? Are its servers and network equipment protected by uninterruptible power supply units located in secure locations and replaced every three years?
- *Cybersecurity*. Does your company have proper cybersecurity software? Does it train its employees on how they can identify phishing attacks?
- *Compliance*. Does your company apply regular server and workstation security patches and updates? Does it perform network vulnerability scans to ensure compliance with federal and state requirements?
- *Backup and disaster recovery*. Does your company proactively monitor its server and cloud infrastructure for performance issues? Does it perform regular backup recovery testing? Does it have a well-defined disaster response team with clearly defined roles, responsibilities, and communication protocols?
- *Business strategy*. Does your company's management team view technology as a worthwhile investment? Does it perform regular technical alignment assessments to determine which areas aren't meeting best practices? Does it have a clear process for making IT-related decisions?
- *Cloud*. Does your company utilize a secure cloud-based email solution? Are your cloud services configured according to the service provider's recommended best practices? Are your cloud-based email and file services configured with data loss prevention policies and alerts to prevent data breaches?

Business Planning and Analysis

For your business to grow and remain competitive in the future, you must develop the right technology plan today. The following tools can help you to create such a plan:

- *Pro forma*. Forecast your company's financial future by creating a pro forma, which anticipates company sales, expenses, cash flow, and balance sheet statements in various potential scenarios. Always err on the side of caution by halving anticipated sales and doubling anticipated expenses.
- *Hardware and software lifecycle inventory*. Identify your hardware and software's estimated lifespans according to their creators. Next, create a spreadsheet that details when each piece of hardware and software was purchased, how long their manufacturers will provide support, when their warranties expire, and when they'll need to be replaced.
- *An IT budget*. Assess your hardware and software lifecycles inventory to estimate how much your company will pay in the upcoming year for new equipment, software licensing, and subscriptions. If you're planning on hiring more people, consider the costs of purchasing more laptops and software subscriptions for them.
- *A technology leadership team*. Assemble a group of managers to oversee all of your company's technologies. Make them responsible for understanding the company's digital needs and how it can best use these technologies to achieve its goals.

Internal Cybersecurity

The most significant risk to your company's cybersecurity is its employees' digital behavior.

To mitigate this issue, you must create an acceptable use policy (AUP) informing employees how they can use the company's technologies safely. Next, hire IT professionals to put the necessary systems and blocks in place to ensure that everyone complies with the AUP. Your company's AUP should define the following:

- Whether employees can use their own devices to access the company's systems.
- If there's a blacklist of websites that employees must avoid.
- If the company will monitor employees' web and technology usage.
- If employees are allowed to use removable drives at the office.
- If employees can use company systems for personal use.
- What data requires encryption across the network.

No single piece of software or hardware can protect your company against the many types of cyber threats. Therefore, you must install a collection of cybersecurity tools—with each designed to defend against a different, specific threat. Such tools might include antivirus software that uses heuristics and databases to detect malware or *endpoint detection and response (EDR)*, a technology that monitors and identifies suspicious behavior and activities at your networks' endpoints.

To determine what other types of protection you need, ask yourself the following questions:

- What information, if lost or stolen, would damage our company's standing with its customers or market? How is this information currently being protected?
- Are our computer and network systems partitioned so that guests only have limited access to restricted designated areas?
- Do all employees have access to the most sensitive data, or just a few?

External Cybersecurity

Don't assume that no one wants to steal your company's data—all data has value. To protect against hackers, you must:

- Require employees to use long, complex alphanumeric passwords across all company devices and systems.
- Hire a skilled network administrator to install a *firewall*, or software that gatekeeps all inbound and outbound connections to the company's devices and networks. Firewalls must be regularly updated and can help prevent devastating denial of service (DOS) attacks, which can render your computers and networks unusable.
- Ensure there's full-device encryption on all company computers.
- Require remote wipe capabilities on devices that leave the office, like employees' work phones, so that email administrators can erase company data from them if they're ever lost or stolen.
- Keep your systems' software and *firmware*, which is the software installed in hardware, up to date.
- Hire IT professionals to periodically review your network's open ports and disable unnecessary access points.

- Install security information and event management (SIEM) software to help your company detect, analyze, and respond to security threats.

Social Engineering

To solicit sensitive information from their targets, hackers often use *social engineering*, or the strategy of exploiting people's tendency to believe what others are telling them. Hackers accomplish this by scraping data about their targets from public websites before *phishing*—sending them an email or text that looks like it's from a legitimate person who knows them. Since social engineering techniques can circumvent cybersecurity systems, you must:

- Train your employees on how to spot these scams.
- Establish a company policy to always decline outsiders' requests for information until their authenticity is verified.
- Enroll your company in a cybersecurity liability insurance plan that covers any losses from social engineering attacks.
- Install advanced phishing detection systems.

Physical Security

The physical security of your company's hardware is as important as its cybersecurity. To keep your equipment safe and functional:

- Have IT professionals conduct regular checkups.
- Ensure that all company hardware has warranties and backup power supplies.
- Calculate the backup batteries' runtimes to determine how much power would be available in an emergency.
- Keep your servers and other network equipment in a separate, temperature-controlled environment where they won't overheat.
- Set up cameras and other surveillance devices to prevent people from tampering with equipment.
- Ensure that only fully vetted individuals can access your company's control systems and critical hardware.

Network Design and Business Continuity

When choosing the right Internet service for your company, you must consider three factors:

1. *Speed, bandwidth, and throughput*: The maximum amount of data that can be transmitted through your Internet connection at any given time.
2. *Symmetric versus asymmetric*: Symmetric Internet connections have equal upload and download speeds, while asymmetric connections have faster download speeds than upload speeds.
3. *Latency*: The measure of how long a standard packet of data takes to travel to and from your connection to another Internet location.

Once you determine which factors are the most important to your company, you can choose the right Internet service. If you have a large workforce and in-house servers, for example, you should prioritize speed and latency. If you have a medium-sized office that primarily uses cloud services, choose the Internet service with the best symmetric connections and latency.

Business continuity systems are tools that help your company keep operating during crises. They're defined by their *recovery point objective (RPO)*, which is the maximum amount of time between a system failure and the company's last systems backup, and their *recovery time objective (RTO)*, the maximum amount of time between a system failure and the company returning to normal operations. The best business continuity systems have onsite servers that frequently take snapshots of the company's operational data before storing them in offsite locations. This results in a low RPO and RTO, allowing companies to quickly return to their normal operations.

Workforce Management

When your team becomes remote, new technologies are needed to keep it running smoothly. There are four areas where such technologies are needed:

1. *Communication*. Synchronous software applications like Zoom and Slack allow employees to keep discussing work in real time, even if they're not in the office together.
2. *Collaboration*. Cloud-based technologies like Google Workspaces help employees simultaneously collaborate on files and documents from different locations.
3. *Virtual desktop*. For companies that have noncloud-based line-of-business applications, technology solutions like Windows Virtual Desktop can help employees access their desktops, programs, and files safely from any device anywhere in the world.
4. *Team engagement*. Microbonus systems allow managers and employees to recognize their colleagues' hard work publicly. Online interactive games can also foster virtual team bonding and engagement.

Business Accounting Systems

It's important to select the right accounting system for your company. An effective system:

- Fits your company's size and growth trajectory.
- Allows you to track and measure your company's performance over time.
- Generates regular financial reports, including profit and loss statements, balance sheets, and cash flow statements.
- Informs employees on how well they're meeting the key metrics for which they're responsible.

Examples of common accounting systems include:

- *Intuit QuickBooks Online*: Cloud-based system best for small companies with fewer than 50 employees and remote teams.
- *Intuit QuickBooks Desktop*: Best for small companies that operate from one location and, therefore, can store their accounting data on an onsite server.

- *Microsoft Dynamics 365*: Enterprise resource planning (ERP) management system best for big companies. ERP systems offer everything from general ledger accounting to customer relationship management, manufacturing resource planning, and operations management.

Laws and Compliance

Companies process and store a great deal of sensitive information, which is why there are laws and regulations to guide their behavior. Although these regulations vary across industries, there are some common ones your company should comply with, including the following:

- The *payment card industry data security standard (PCI DSS)* is a set of industry standards that all credit card processors must follow to accept and store credit card information.
- The *red flags rule* is a regulation that requires companies to implement identity theft programs to protect their consumers' information and to report any incidents of identity theft to the individuals affected by it.

Documentation, Policies, and Procedures

It's critical to document your company's important information so that it exists outside of employees' minds. Such information may include its processes, policies, marketing content, vendor lists, pricing processes, business software, and intellectual property.

Documentation provides tools to educate and train other employees while also increasing the value of your company's business. It's important to categorize these documents by classification levels, including publicly accessible, confidential, and highly restricted with full encryption. This will restrict who can access sensitive information and help protect the company against hackers and competitors.

About the Author

Nathan Whittacre founded Stimulus Technologies in 1995 with his brother and father with a goal to provide advanced technology solutions for his clients. His passion for innovation, analyzing hard issues, creating solutions, and fixing problems has created a portfolio with a wide variety of information technology skills. A published author with over 30 years' experience in technology and entrepreneurship, he brings his passion in helping people better their lives through technology, cyber security, and intentional culture.

Purchase the Book