PLANO CHAMBER OF COMMERCE

CYBERSECURITY GUIDE

FOR SMALL & MID-SIZED BUSINESSES

SPONSORED BY

Kehr Technologies
Solutions that power your business.

FLAIR DATA SYSTEMS
EST. 1916

CYBERSECURITY GUIDE
FOR SMALL & MID-SIZED BUSINESSES

TABLE OF CONTENTS

PROJECT SPONSORED BY:

Kehr Technologies
Solutions that power your business.

FLAIR DATA SYSTEMS
EST. 1916

PROJECT CONTRIBUTORS:

EMILY BELL-WOOTTEN, AUTHOR & PROJECT LEAD
FLAIR DATA SYSTEMS

BOB KEHR, PROJECT SPONSOR
KEHR TECHNOLOGIES

NATE HOWE, CISO
THE UNIVERSITY OF TEXAS AT DALLAS

GABRIELLA PATE, DIRECTOR-GOVERNMENT & COMMUNITY RELATIONS
THE UNIVERSITY OF TEXAS AT DALLAS

RICHARD SERNA, SOLUTIONS ADVISOR
FLAIR DATA SYSTEMS

This entire publication and it's contents are © 2024 Plano Chamber of Commerce, all rights reserved. The information in this Cyber Security Guidebook is for general informational purposes only. While we strive for accuracy, we make no warranties about the completeness, reliability, or suitability of the content. Any reliance on this information is at your own risk. The Plano Chamber of Commerce will not be liable for any loss or damage arising from the use of this Guidebook. Links to external sites are not endorsed, and we are not responsible for their content. Readers should seek professional advice for specific cybersecurity issues.

PLANO CHAMBER OF COMMERCE

5400 Independence Pkwy, STE 200
Plano, Texas 75023
972.424.7547 | PLANOCHAMBER.ORG

THE WHY?

A Message from the **Plano Chamber of Commerce**

Welcome to the world of cybersecurity, where every digital interaction is a potential battleground, and every organization, regardless of size, is a potential target. As we navigate the complexities of the digital age, understanding and implementing effective cybersecurity measures are paramount to safeguarding our businesses, our livelihoods, and our future.

The Plano Chamber of Commerce, in collaboration with Flair Data Systems, Kehr Technologies, and The University of Texas at Dallas (UTD), is pleased to introduce this comprehensive guide on cybersecurity. Designed to serve as a practical resource for small to mid-sized businesses, this guide aims to demystify the intricacies of cybersecurity and empower organizations to protect themselves against ever-evolving cyber threats, whatever your size. While risk can never be fully eliminated, this manual will help any organization improve its risk management and mitigation capabilities.

As we embark on this journey together, I encourage you to approach cybersecurity not as an isolated concern but as an integral part of your overall business strategy. By prioritizing cybersecurity and investing in proactive measures, we can collectively strengthen our defenses and protect the prosperity and vitality of our Plano business community for years to come.

Thank you for joining us on this important journey!

Kelle Marsalis

Kehr Technologies
Solutions that power your business.

FROM OUR SPONSORS

Kehr Technologies recognizes the critical importance of cybersecurity for businesses of all sizes. That's why we've partnered with the Plano Chamber of Commerce to create this Cyber Security Guide, designed to provide businesses with straightforward protection strategies.

Our goal is to help businesses balance security and productivity. This guide outlines key threats, beneficial measures, and services to enhance protection while fostering a culture of security. Remember, the most crucial layer of protection is an informed user.

As a long-time Plano Chamber member, Kehr Technologies is committed to helping businesses tackle cybersecurity challenges. We support our clients with training, advanced IT solutions, and a friendly support team.

Make the most of this guide, which offers simple, practical protection methods. If you need further assistance, Kehr Technologies is here to help.

Bob Kehr
Owner/Chief Technical Officer
Kehr Technologies | https://www.kehrtech.com/

FLAIR
DATA SYSTEMS
EST. 1916

Flair Data Systems is happy to announce the launch of the Cybersecurity Manual and thank the Plano Chamber of Commerce for asking us to join them on this mission to help Plano Businesses protect what's important. For us, this has been a labor of love and necessity. With cyber threats exponentially increasing, we could see that our small business community would be impacted by cybercrime but may be oblivious to the Monster lurking in the room.

Partnering with the Plano Chamber of Commerce underscores our commitment to supporting the local business community in navigating the complex landscape of cybersecurity. Flair Data Systems understands the critical importance of cybersecurity in today's interconnected world. With our expertise in providing cutting-edge IT solutions and cybersecurity services, we have witnessed firsthand the profound impact that effective cybersecurity practices can have on businesses, from enhancing resilience to mitigating risks and ensuring operational continuity. Together, we recognize the shared responsibility we have in promoting cybersecurity awareness and fostering a culture of cyber resilience among businesses in our community.

We hope you find this manual a valuable resource for your business. Please reach out and let us know how we can support you.

Bob Burgess- President and Robert Burgess- VP Technology
Flair Data Systems | https://www.flairdata.com/

SAFEGUARDING YOUR SMALL BUSINESS

Navigating Cybersecurity

An organization loses

$4.8 MILLION

in the average data breach

IBM SECURITY REPORT

Cyber-attacks on small businesses are increasing, with significant financial and reputational damage from data breaches and ransomware. Small businesses are often seen as easy targets due to limited resources and security measures. As more businesses go digital, the risk of cyber-attacks is higher than ever, with threats like phishing and malware posing serious risks. It’s estimated that 43% of cyber-attacks target small businesses, underscoring the need for strong cybersecurity measures.

Cybersecurity Guide Checklist

In our digital age, cyber threats are everywhere, and no one is off the radar — not even the smallest of businesses. When cyber-attacks happen, it's more than just a technical headache, you can be held liable for wrongfully accessed data, and it can bleed your finances. Worse, it can make your customers lose faith in you. Can you afford to possibly lose your business? This Cybersecurity Checklist isn't just a bunch of steps; it's your battle plan for keeping your business safe and your customers' trust intact.

Securing your most vital resource - PEOPLE

- □ Help employees understand that criminals will target your organization.
- □ Remember that good customer service includes protecting data.
- □ Consider establishing an Acceptable Use Policy detailing your expectations about data, personal devices, and next steps if the employment relationship ends.

Secure Your IT

- □ Rapidly apply software patch updates to all business and personal devices.
- □ Provide each employee with the least access needed to do their work. When they leave employment, disable access rapidly.
- □ Be thoughtful about Wi-Fi registered to your business. If someone commits a crime using your connection, you could be visited by law enforcement.
- □ When disposing of an IT device, be sure the data it contains has been erased.

Criminals will interrupt your business and charge for access to your own computers.

- □ Back up important data. Working backups allow you to recover from a ransomware attack without paying criminals.
- □ Regularly purge electronic data that is no longer needed, as this reduces your exposure if hacked.
- □ Meet with your team to discuss offline work procedures to follow when IT outages eventually occur.

Cloud providers can simplify IT.

- □ Rather than purchasing IT equipment that is expensive and difficult to maintain, subscribe to reputable cloud providers to meet your needs.
- □ Adjust your cloud services based on seasonal capacity needs.
- □ Seek security commitments during the contracting process.
- □ Understand the benefits and risks of generative artificial intelligence (AI) services before allowing company data to be uploaded.

Social media management is critical to your brand reputation.

- □ Understand what has been posted about your organization and seek to correct errors.
- □ Ensure that you protect your official social media accounts with complex, long passphrases.
- □ Be sure that you can manage your social media accounts even if particular employees leave the organization.

Physical security matters too.

- □ Locked facilities, intrusion alarms, and cameras.
- □ Use locks to protect IT equipment and paper records from theft.
- □ Shred paper records before disposal.

Seek professional advice from an attorney or Cybersecurity expert.

- □ You may be required to comply with specific requirements based on your industry or contracts.
- □ Cyber insurance is available to help with the costs of incident response.
- □ Visit **PlanoChamber.org** and use our Business Directory to search for IT Professional Service Providers.

Strive for Resilience

- □ Cross train employees in case some become unavailable.
- □ Consider how remote work and paperless processes might enable operations to continue throughout a disruption.
- □ Establish reciprocal agreements with other organizations.

FIND A CYBERSECURITY EXPERT
Our Business Directory features trusted professionals who specialize in Cybersecurity, Visit **members.planochamber.org** or Scan the QR Codefor more info.

In Collaboration with **The University of Texas at Dallas**

THE UNIVERSITY OF TEXAS AT DALLAS UTD EST. 1969

PLANO CHAMBER OF COMMERCE

STATISTICS

The cost of Cybercrime is projected to reach a staggering $10.5 TRILLION by 2025

The following list includes some alarming statistics and potential risks facing companies today:

· The cost of cybercrime is projected to reach a staggering **$10.5 trillion** by 2025.

• The average cost of an organization detecting and escalating a data breach is **$1.58 million**.

· Did you know that cybersecurity is a big deal for people and businesses everywhere, not just in the U.S., but globally? California, Florida, New York, **Texas**, and Georgia are the top five hit by cybercrime when it comes to money lost. (Cybersecurity Stats: Facts And Figures You Should Know – Forbes Advisor)

· **Phishing attacks** remain one of the top cybersecurity threats. Roughly **90%** of data breaches begin with phishing a vulnerable employee. According to the Federal Bureau of Investigation, phishing attacks may increase by as much as 400% year-over-year.

· **Ransomware attacks** have increased with businesses of all sizes being targeted, costing an estimated average of **$650,000**, though the actual median ransomware payment was 46% less at $350,000, according to the "2023 Unit 42 Ransomware and Extortion Threat Report."

· Insider threats remain a major concern, accounting for **60%** of reported data breaches, with malicious insiders and **negligent employees** being the primary sources of insider-related security incidents. A data breach costs $4.45 million on average. IBM Cost of a Data Breach Report 2023

· **Email remains the predominant channel for malware distribution, with approximately 35%** of malware being delivered via email in 2023 (Verizon 2023 Data Breach Investigation Report). An alarming **94%** of organizations have reported email security incidents (Egress 2024 Email Risk Security Report). Moreover, business email compromises resulted in staggering losses totaling $2.7 billion in 2022 alone (FBI Internet Crime Report 2022).

· Cloud (which comprises most of the technology used by small business) security incidents are a concerning trend. According to the IBM X-Force Cloud Threat Landscape Report 2023, there was a **194% increase** in new cloud-related vulnerabilities (CVEs) between June 2022 and June 2023 compared to the previous year- Cloud CVEs Surge 200% in a Year - Infosecurity Magazine (infosecurity-magazine.com)

TYPES OF CYBER ATTACKS

PHISHING & SMISHING

Phishing attacks, where cybercriminals trick users into revealing sensitive information, are one of the top cyber-attacks facing small businesses. Smishing combines SMS and phishing, targeting mobile devices with unwanted text messages.

Other types: Spear Phishing

MALWARE

Malicious software (malware) poses a significant risk. It comes in various forms, including viruses, Trojans, and spyware.

Other types: Ransomware: This type of malware encrypts data to make it unusable to the victim and demands payment for decryption, with the promise of restoring the system and data to a useable state. Small businesses are often targeted.

VULNERABLE WEB APPLICATIONS

Misconfigured, unpatched, and poorly designed applications available on the Internet (for example, your company's website) can be exploited by anyone in the world. Your weakness could become a path to your internal network and most valuable records. Specialized testing of web applications is needed to identify flaws and develop stronger coding practices.

INSIDER THREATS

Sometimes, the most dangerous actors come from within an organization. There are even reports of cyber criminals approaching employees and offering to split the proceeds of an attack, if the employee will participate in helping the attacker successfully extort a ransom.

TYPES OF CYBER ATTACKS CONT.

FRAUD & IDENTITY THEFT

Cybercriminals steal personal information for financial gain.

DENIAL OF SERVICE (DOS) ATTACKS

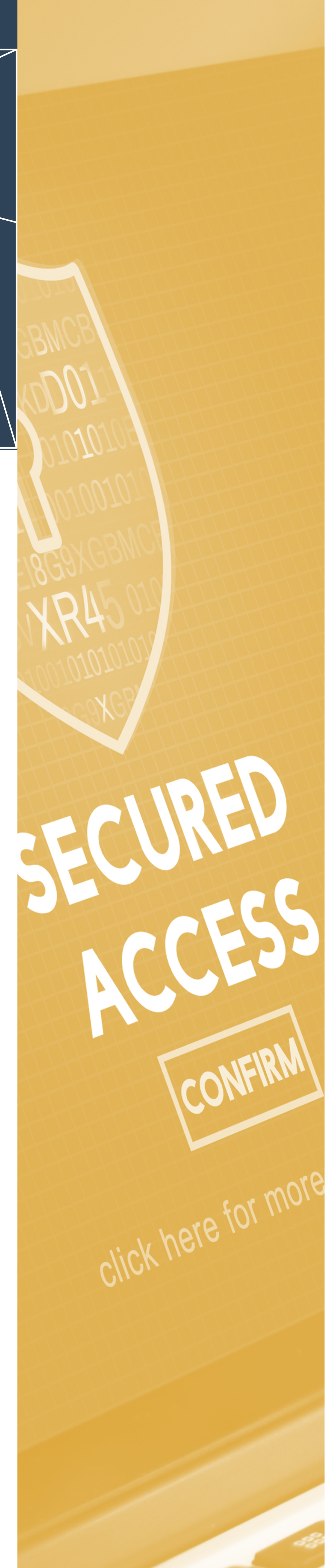
These types of attacks overload systems, disrupting services, and are one of the most prevalent attacks across all sizes of business.

SUPPLY CHAIN ATTACKS

Targeting third-party vendors or partners can compromise a business's security.

DATA BREACHES

Unauthorized access to sensitive data can lead to severe consequences. This includes unauthorized parties gaining access to sensitive or confidential information including personal and corporate protected data (Social Security numbers, banking information, healthcare data, etc.),



PREVENTING CYBER ATTACKS

As a small business owner, understanding the different types of cyber attacks and how to prevent them is crucial for safeguarding your business. Stay informed, stay prepared, and protect your business from potential threats. Your efforts in maintaining robust cybersecurity practices will not only protect your data but also preserve the trust and loyalty of your customers.

- DEVELOP CYBER SECURITY MEASURES
- IMPLEMENT DATA BACKUP
- CONDUCT EMPLOYEE TRAINING & AWARENESS
- CREATE AN INCIDENT RESPONSE PLAN
- PERFORM CYBER SECURITY AUDITS
- PROTECT IMPORTANT INFORMATION
- MANAGE THIRD-PARTY VENDORS/SUPPLIERS
- INITIATE CREDIT FREEZES & MONITORING SERVICES
- SET UP FRAUD ALERTS
- REVIEW FINANCIAL STATEMENTS REGULARLY
- OBTAIN CYBER INSURANCE

SO, YOU HAVE BECOME A VICTIM. NOW WHAT?

IT CAN HAPPEN TO YOU!

As a small business owner, you might think you are immune to cyber threats, but the reality is that no one is too small to be targeted. Cybercriminals often see small businesses as easy targets due to limited resources and inexperience with security measures.

The following section outlines preventive measures you can take to secure your business, while providing a step-by-step guide on what to do during a cybersecurity compromise.

FIRST STEPS

1. Obtain guidance from a licensed attorney experienced with security and breach notification (organizations suffer many types of cyber incidents, but not all are treated as reportable breaches – an attorney can help you sort through requirements specific to your industry)

2. Contact technology provider/security consulting firm(s) equipped to support your incident response efforts

3. Strongly consider avoiding paying ransoms to cybercriminals, as this emboldens them and could lead to further attacks across the economy

4. Contact law enforcement

5. Investigate your liability

6. Disclose or Not to Disclose? Know when and who to tell about data compromise.

LIABILITY AND REPORTING: NEXT STEPS

What is your liability if identity theft, breach, or data theft occur due to a system failure or weak process within your business? Here is a checklist of next steps when an individual or a company experience a cybersecurity breach:

STEP 1 | CONTAIN THE INCIDENT

o Isolate affected systems

o Disconnect compromised systems from the network

STEP 2 | ASSESS THE DAMAGE

o Identify the type of incident and scope of the damage; in consultation with an attorney, determine if a reportable data breach has occurred

o Determine what data or systems were affected

STEP 3 | NOTIFY RELEVANT PARTIES

o Inform internal stakeholders and executive management

o Notify affected customers and partners, as appropriate based on attorney guidance

o Report the breach to relevant authorities and regulatory bodies, as appropriate based on attorney guidance

STEP 4 | INVESTIGATE THE INCIDENT

o Conduct a forensic investigation to determine the cause and method of the breach

o Collect and preserve evidence for analysis

FIND A CYBERSECURITY EXPERT
Our Business Directory features trusted professionals who specialize in Cybersecurity, Visit **members.planochamber.org** or Scan the QR Codefor more info.

STEP 5 | MITIGATE THE THREAT

- o Apply necessary patches and updates
- o Remove malware and unauthorized access
- o Strengthen security controls to prevent recurrence
- o Format and reinstall IT systems to ensure that malware and threat actors are fully purged

STEP 6 | COMMUNICATE EXTERNALLY

- o Prepare a public statement, if required
- o Manage public relations and media inquiries

STEP 7 | RECOVER AND RESTORE SYSTEMS

- o Restore data from trusted backups, preferably those taken before the system compromise occurred
- o Verify the integrity of restored systems
- o Resume normal operations

STEP 8 | REVIEW AND IMPROVE SECURITY MEASURES

- o Analyze the incident to identify weaknesses
- o Update security policies and procedures
- o Provide additional training to employees

STEP 9 | DOCUMENT THE INCIDENT

- o Create a detailed report of the breach, actions taken, and lessons learned
- o Maintain records for compliance and future reference

STEP 10 | FOLLOW UP

- o Monitor systems closely for any signs of further compromise
- o Conduct regular security audits and assessments
- o Discuss lessons learned with organization leaders and IT staff to further refine procedures
- o Conduct periodic incident exercises and incorporate lessons learned from previous incidents
- o Format and reinstall IT systems to ensure that malware and threat actors are fully purged

STEP 11 | DISCLOSURE

Disclosing a cybersecurity breach to the public or law enforcement involves understanding regulatory requirements and best practices. Here are the key considerations:

When to Disclose a Breach

Regulatory Requirements:

o **Federal Regulations:** The Gramm-Leach-Bliley Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA) require notification of data breaches involving financial and health information, respectively.

o **State Laws:** Most states have data breach notification laws that mandate disclosure to affected individuals and, in some cases, state regulators within a specific timeframe (typically 30 to 90 days) after discovering a breach.

o **General Data Protection Regulation (GDPR):** If operating in the EU, GDPR requires notification of personal data breaches to the relevant supervisory authority within 72 hours and to affected individuals without undue delay.

o **Securities and Exchange Commission (SEC)** new rules introduced in 2023 require Board of Directors oversight of cybersecurity and reporting of incidents which may be material to financial performance, in as little as four business days, for publicly traded companies.

Federal Bureau of Investigation (FBI) Notification:

o **Immediate Threats:** Notify the FBI if the cyber incident involves a significant threat to national security, critical infrastructure, or significant financial fraud. Go to www.ic3.gov for more information.

o **Legal Obligations:** Certain incidents, especially those involving ransomware, espionage, or attacks from foreign entities, are considered breaches and require notification under federal laws.

o **Contact Methods:** Use the FBI's Internet Crime Complaint Center (IC3) at www.ic3.gov for online reporting or contact the local FBI field office directly.

o **Information to Provide:** Include a detailed account of the breach, types of data affected, suspected source of the breach, and any steps taken to mitigate the impact.

How to Disclose a Breach To the Public:

o **Notification Methods:** Use multiple channels (email, website notices, press releases) to reach affected individuals promptly.

o **Content of Notification:** Include details about the breach (what happened, what data was affected), steps taken to mitigate the breach, and recommendations for individuals (such as monitoring accounts or changing passwords).

GLOSSARY

What is cybersecurity?

Cybersecurity refers to protecting information assets from disruptions to confidentiality, integrity, and availability. These three objectives, sometimes referred to as the "CIA triad," simply mean that your information should only be observed by those with a legitimate need, should not be altered unless such changes are legitimate, and needs to be useable and efficient in the operation of your business.

Cybersecurity can be categorized into five distinct types:

Application security- Application security focuses on protecting software applications from threats by reducing vulnerabilities introduced throughout their development lifecycle. Key components of application security include:

- Authentication and authorization
- Data input validation
- Encryption
- Error handling and logging
- Patch management
- Penetration testing and code reviews
- Secure coding practices
- Secure configuration management
- Secure deployment practices
- Session management

Cloud security- Don't let the term "cloud" confuse you. This refers to using IT services hosted by a business partner and accessed via the Internet. These services are usually delivered in a subscription model and can be adjusted rapidly to meet the needs of your business. Though you may use cloud services that are owned by your business partner, remember that your ownership rights to your data follow it into the cloud service. Cloud security encompasses various technologies, processes, and controls designed to protect data, applications, and infrastructure hosted in cloud environments.

Critical infrastructure security- involves protecting the systems, networks, assets, and facilities that are essential for the functioning of a society and economy.

Internet of Things (IoT) security- IoT security encompasses various practices, technologies, and protocols designed to protect Internet of Things (IoT) devices and networks from cyber threats.

Network security- Network security refers to the practices and measures adopted to protect the integrity, confidentiality, and availability of data and resources within a computer network. Network security aims to secure both the internal network infrastructure (such as routers, switches, and servers) and the data transmitted over the network (such as emails, files, and communications).

RESOURCES

Businesses Must Provide Victims and Law Enforcement with Transaction Records Relating to Identity Theft Link

2023 Business Impact Report- idtheftcenter.org

Cisco Secure Small Business Solutions (Flair Data Systems- reseller)

Small Business is a Big Priority: NIST Expands Outreach to the Small Business Community

Flair Data Systems: Cybersecurity and Tech Insights Blog

Kehr Technologies: Tech Insights Blog

UTD Cybersecurity Assessment Application (Apply at: infosecurity@utdallas.edu)

Internet Crime Complaint Center (IC3)

Federal Trade Commission: Data Breach Response: A Guide for Business

NAIC Cybersecurity Insurance Guidelines

SBA.gov Cybersecurity

National Cybersecurity Alliance

Texas Data Privacy and Security Act

On March 6, 2023, National Institute of Standards and Technology (NIST) launched a new small business initiative that will create more opportunities for the exchange of information, resources, and ideas between NIST and the nation's small business community via the creation of a new Small Business Community of Interest.

NIST Small Business Cybersecurity Act, which directed us to "disseminate clear and concise resources to help small business concerns identify, assess, manage, and reduce their cybersecurity risks." This resource repository has grown over the years and offers videos, planning guides, case studies, topical guidance (e.g., ransomware, phishing, and teleworking), and important information that small businesses can put into action.

FIND A CYBERSECURITY EXPERT
Our Business Directory features trusted professionals who specialize in Cybersecurity, Visit **members.planochamber.org** or Scan the QR Codefor more info.

NOTES

NOTES

PLANO CHAMBER OF COMMERCE

SPONSORED BY

Kehr Technologies

Solutions that power your business.

FLAIR DATA SYSTEMS

EST. 1916