THE 20

Cratin Computing

CYBERSECURITY

Protect your data with a proactive approach against cyberattacks

EXECUTIVE SUMMARY

When's the last time you didn't have your phone? What happens to your office when the network goes down for just a matter of minutes?

Our lives and our businesses have gone digital. As a result, the importance of cybersecurity constantly grows stronger.

When developing a cybersecurity action plan to keep your data safe, it's critical to know the how and the why. This ebook will explore what cyberattacks are, what the after effects are and how they can be prevented.

Takeaways include:

- Impact on small to mid-size businesses
- 10 of the most common cyberattacks
- A deep dive into the Dark Web
- Clues that someone has stolen your information
- Multi-layered cybersecurity approach
- Proactive measures to securing data

Cratin Computing THE 20

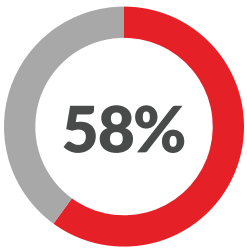
TABLE OF CONTENTS

VALUE OF CYBERSECURITY

A cyberattack is a deliberate exploitation of computer systems, technology-dependent enterprises or networks.

Cyberattacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft.[1]

Cyberattacks aren't only affecting gigantic banks and corporations .



58% of data breaches hit small businesses in 2017. That's up from **53%** in 2015.[2]

A smaller business does not mean smaller vulnerability. Whether a hacker seeks financial gain or just wants to watch the world burn, an easy target is appealing. That's what makes cybersecurity so valuable.

The devastation is real. Cyberattacks typically cost small businesses **$84,000 – $148,000**.[3] That's real money… gone. It's often too much to handle.

Nearly 60% of small businesses shut down after a cyberattack.[4]

So you should just throw your hands in the air and shut the doors, right?

Of course not. But you should take cybersecurity seriously.

Understanding what a cyberattack is and how a cyberattack occurs is key in developing a cybersecurity plan to keep your data safe.

HOW HACKERS ATTACK

Businesses store critical data on their systems. Financial accounts, customer records, proprietary information — it's all at risk if your data is compromised.

Personal information could also be involved, meaning passwords, credit card numbers, medical records, etc. could fall into the wrong hands.

It helps to be familiar with the most common cyberattacks being used on networks and individuals.

We'll also take a look at a haven for malicious activity, the Dark Web.

10 COMMON CYBERATTACKS

Cyberattacks are ever evolving. However, there are similar schemes and tactics that attackers use when they try to hack an individual or organization.

Most hackers don't want to reinvent the wheel; they want to use what they know. Here's a look at some of the most common cyberattacks being used today.

Malware
Short for "malicious software," malware is intentionally designed to damage or disable a computer or entire system. It's a catch-all for other terms you may have heard, such as worms, Trojan horses, ransomware, spyware and adware.

Spyware
Software that enables an attacker to obtain covert information about another's computer activities by transmitting data from their hard drive.

Ransomware
A form of malware that attackers use to hijack your system and demand a ransom. They'll block your access or threaten to release your information unless a payment is made.

Pharming
Fraudulently directing web users to a bogus website that looks legitimate in order to obtain personal information. You should only download files or submit forms on websites that you trust.

Phishing
Fraudulently sending emails appearing to be from reputable companies in order to induce individuals to reveal personal information. If an email looks strange (or... fishy), just delete.

Virus
A piece of code that is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data. Utilize pro-grade anti-virus software and make sure it stays updated.

Password Sniffer
An application that listens to all incoming and outgoing network traffic and records any instance of a data packet that contains a password.

Password Attack
Software that attempts to guess a user's password through methods like brute force (a large number of consecutive guesses) or a systematic word combinations. Malicious code isn't even required because attackers can use their own system. Strong password policies are the best safeguard.

Denial-of-service
An interruption in an authorized user's access to a computer network, typically caused with malicious intent.

Website Defacement
One of the most popular cyberattacks is simply hackers wreaking havoc. Unauthorized changes to a website's appearance tarnish a company's brand and can cost considerable amounts of time and money to resolve.

WHAT IS THE DARK WEB?

The Dark Web... sounds haunting, doesn't it? While accessing the Dark Web requires specific knowledge and systems, its reach can be quite perilous.

The Dark Web is ripe with malicious activity so it's important to understand what's out there. The world wide web basically consists of 3 parts:

- **The Surface Web** is everything that's publicly available and accessible through search engines or typing a URL into your browser.
- **The Deep Web** is all the content on the web that is not indexed by standard search engines, such as email clients and online banking websites.
- **The Dark Web** refers to heavily-encrypted sites that cannot be accessed with your average, run-of-the-mill browser. As a result, these sites are often used as a black market, and as a source for hacked data.

The main characteristic of the Dark Web is its anonymity.

The Dark Web is widely used as an instrument for illegal activities as a result. These activities include child pornography, drug dealing, firearm sales and trading stolen credit card numbers.

The most famous example of illegal Dark Web activity is Silk Road, which used a combination of Bitcoin and the Dark Web to exchange drugs internationally. Law enforcement agencies took down the online marketplace in 2013 and arrested its alleged founder — and again, in 2014.

All the common dangers of a traditional black market exist on the Dark Web. However, there are also some unofficial dangers to consider.

WHAT IS THE DARK WEB?

Many of those who operate in the Dark Web have no problem exploiting you in any way they can — and since many of them are hackers or at least know how to use hacking tools, they can be dangerous.

As a result, there are many tales of blackmail peppering the Dark Web. Downloads also tend to be even more suspect in the dark corners of the Internet, so your computer may be in danger as well.

Frightening, isn't it? A bit overwhelming? It's important to be aware of what is going on in order to prevent unauthorized access.

▶ In the next couple of chapters we'll look at what happens when a cyberattack strikes and measures you can take to protect yourself and your business from the Dark Web and cyberattacks in general.

10 most common pieces of information on the Dark Web[5]

- Social Security number: **$1**
- Credit or debit card: **$5-$110**
- Online payment services login info (e.g. Paypal): **$20-$200**
- Loyalty accounts: **$20**
- Subscription services: **$1-$10**
- Diplomas: **$100-$400**
- Driver's license: **$20**
- Passports (US): **$1,000-$2,000**
- Medical records: **$1-$1,000**
- General non-financial institution logins: **$1**

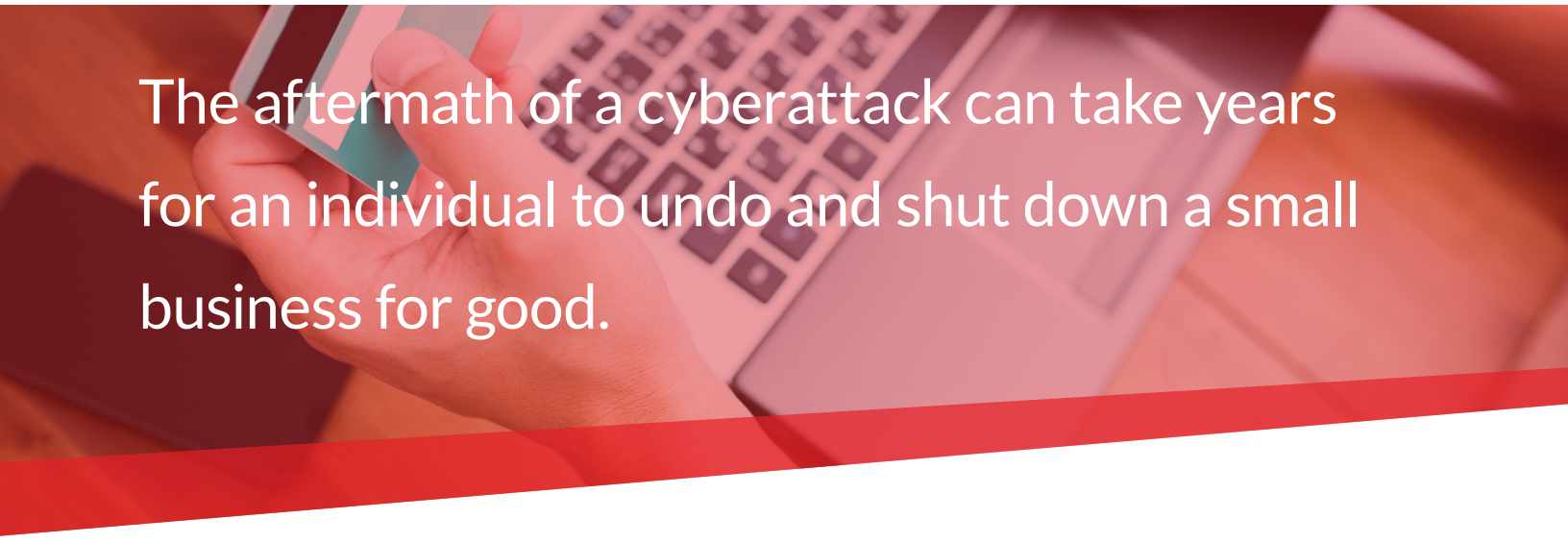
AFTERMATH OF A CYBERATTACK

Equifax – 143 million consumer accounts compromised in a massive 2017 data breach. Equifax extended offers of free credit monitoring to affected consumers, but would you really want to take them up on that?

Yahoo – 3 billion user accounts compromised in 2013, the biggest known data breach to date. The once dominant Internet giant would eventually be sold, for hundreds of millions ...less than anticipated.[6]

Attackers even went after Chili's! Brinker International, which operates over 1,600 Chili's restaurants globally, announced the data breach in 2018. They believe malware was used to gather payment card information including credit or debit card numbers as well as cardholder names.[7]

These are real-life examples of cyberattacks crippling organizations and greatly affecting individuals in a way they won't forget. The impact on a small business is no different.



The aftermath of a cyberattack can take years for an individual to undo and shut down a small business for good.

IDENTITY THEFT

Identity theft is the use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name.

Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax refund in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest.

Data breaches and malware are two of the leading factors of identity theft. A proactive approach to protecting your personal information is paramount.

Clues that someone has stolen your personal information[9]

- You see withdrawals from your bank account that you can't explain.
- You don't get your bills or other mail.
- Merchants refuse your checks.
- Debt collectors call you about debts that aren't yours.
- You find unfamiliar accounts or charges on your credit report.
- Medical providers bill you for services you didn't use.
- Your health plan rejects your legitimate medical claim because the records show you've reached your benefits limit.
- Your medical records show a condition you don't have.
- The IRS notifies you that more than one tax return was filed in your name, or that you have income from an employer you don't work for.
- You get notice that your information was compromised by a data breach at a company where you do business or have an account.

IT DOWNTIME

Infrastructure matters. When your network or applications unexpectedly fail or crash, IT downtime can have a direct impact on your bottom line and ongoing business operations. In some extreme cases, data and monetary losses from unplanned outages can even cause a company to go out of business.

The industry average cost of downtime is dependent on a lot of areas. The monetary losses vary when you consider your revenue, industry, the actual duration of the outage, the number of people impacted, the time of day, etc.

Other costs don't often show up in dollar form. Did you know, according to a study by UC Irvine, that it often takes an average of **23 minutes** to refocus and get your head back in the game after an interruption?[10]

IT downtime affects customer retention, employee productivity and standing in the marketplace. It is extremely expensive, and in ways that can make or break the success of your organization.

Preparing for IT Downtime

So, what can you do? Are there any positives in all of this? The best news — and what really matters — is that simply taking a few steps to prepare for an outage can make a huge difference. You can, for instance, take the time to define which services require the most prioritized response, have contingency plans in place, leverage post-mortems to improve processes, and conduct regular testing.

By taking the time to implement a plan for addressing inevitable downtime, your organization stands to realize thousands of dollars in quantifiable cost savings, as well as ensure the health of crucial qualitative factors such as employee morale, brand reputation and customer loyalty.

PROACTIVE CYBERSECURITY

Numerous types of cyberthreats are circulating the web. The ability to mitigate or prevent attacks relies on an agile, multi-layered approach that can adapt as new and increasingly hostile threats emerge.

A best-in-class proactive approach consists of six layers.[11]

1. Patching

The most basic layer of protection is to monitor and patch all computers and applications. The latest patches can close all known OS Security vulnerabilities. Patching provides the most basic layer of protection to operating systems, especially once a security flaw is uncovered. When clients have the latest patches, they can ensure their operating systems are running at peak performance and that all system vulnerabilities are addressed.

2. Anti-virus and Network Monitoring

People are being targeted through more sources than ever — email, ad networks, mobile applications and devices. Anti-virus and network monitoring examines all files and traffic, and filters them against all known threats. Keeping virus definition files current is critical to ensuring these systems are running at peak performance.

3. Backup and Disaster Recovery (BDR)

There is sometimes a gap between when a threat is first introduced and when a vendor is notified and develops a remedy. Making a full-system backup protects back-office systems when an attack occurs and provides a recovery option for unknown threats and even the most catastrophic failures.

4. Endpoint Backup

Although there's a layer of protection on back-office systems, you still need to have backup and recovery of data for devices. These devices create, share and store business data, and if a cybercriminal captures this proprietary and sensitive information, it can have a significant impact on business productivity and profitability. Enabling real-time data backup on these endpoints can prevent business-critical information from being compromised.

5. Secure File Sync and Share

Allow employees to collaborate securely from any location and using any device — even their smartphones and tablets. Grant access and editing controls for specific documents, such as Word documents, Excel spreadsheets and PowerPoint presentations, and allow employees to recover documents that are maliciously or accidentally deleted.

6. Education and Awareness

IT service providers must educate clients and their employees about cybersecurity risks, new ransomware strains and best practices for spotting phishing attempts, suspicious emails and other security risks. Empowering them to be proactive and encouraging them to report questionable content using rewards and incentives will help increase awareness and decrease overall risk.

PROACTIVE CYBERSECURITY

A proactive cybersecurity approach means taking protective measures to secure your data before a cyberattack happens. It's about keeping data safe, not about having to deal with the aftermath of an attack.

Here are steps you can take to protect your own personal information:

- Maintain healthy password practices
- Don't share your personal information unless it's necessary
- Utilize two-factor authentication
- Make sure that you keep your antivirus software and software updated on all devices (desktop, laptop, tablet, phone)

Securing information is key to data privacy.

Data security can only work in concert with strong preventative policies to back up the technology.

While data security measures can be quite effective, important strategies such as keeping up with patches and utilizing encryption can help ensure that the technology actually works.

Cybersecurity will continue to play a massive role in our businesses and our personal lives.

▶ Our IT Management Platform, 24/7 Support Desk, and Network Operations Center (NOC) are 100% US-based. Our comprehensive services ensure that client information stays secure and in compliance with federal and industry regulations.

What are you doing to keep your data private?

NETWORK SECURITY AUDIT

A Network Security Audit is a great instrument to assess your cybersecurity position. Normally we charge $499 for this service, but as a potential client, we would like to offer this to you for free.

Get answers to questions such as:

Is your business compliant?

You might've heard of data security measures like GDPR (General Data Protection Requirement) or HIPAA (Health Insurance Portability and Accountability Act). Protecting personal information isn't just best-practice anymore, it's required.

Is your WiFi secure?

There are several factors to investigate, including encryption method, how your network and guest network is segmented, updates, patches and more.

Is your password policy strong enough?

A strong password policy is one of the best safeguards against identity theft.

Additionally, during your Network Security Audit we'll come onsite to:

- Pinpoint exposure to cyberattacks, data loss, power outages, downtime, spam, and even employee sabotage. This analysis will assess your risk of identity theft.
- Review your backups to ensure data can be recovered in case of a disaster.
- Assess hidden problems that cause error messages, slow performance and network crashes.
- Answer any questions you have about your network or keeping it running problem-free. We can also give you a second opinion on any projects you are considering.

Knowing your network is secure brings peace of mind and lets you focus on growing your business.

Cratin Computing

Let Us Handle Your IT Services

Whether you have problems to solve today or are looking to head off IT problems tomorrow, you need the right IT partner — one that provides the support you need, is close by, and can grow with you long term.

We've got you covered.

LEARN MORE

or Call Us Today: 215-793-4200

SOURCES

1. Techopedia. Cyberattack Definition.
2. Verizon. 2018 Data Breach Investigations Report.
3. UPS Capital. Think Cybercrime Only Strikes Big Companies? Think Again.
4. Strauss, S. (2017, Oct 20). Cyber threat is huge for small businesses.
5. Stack, B. (2018, Apr 9). Here's How Much Your Personal Information Is Selling for on the Dark Web.
6. Armerding, T. (2018, Jan 26). The 17 biggest data breaches of the 21st century.
7. Kerner, S. (2018, May 14). Chili's Discloses Data Breach Exposing Payment Card Information.
8. Verizon. 2018 Data Breach Investigations Report.
9. Federal Trade Commission. Warning Signs of Identity Theft.
10. Pattison, K. (2008, Jul 28). Worker, Interrupted: The Cost of Task Switching.
11. Autotask. 6 Ways to Shield Your Clients from Ransomware.

Cratin Computing

www.cratin.com
info@cratin.com
215-793-4200

1223 Forsythe Dr.
Ft. Washington, PA

The 20 MSP, LLC www.the20.com