Small Business Cyberattacks You Haven’t Heard Of

Cyber Incidents That Didn’t Make the Headlines

Cyberattacks are commonly thought of as an enterprise-level problem among businesses. The headlines after all typically feature large national or even global organizations, such as Adobe in 2013, Myspace in 2013, CapitalOne in 2018, Best Buy in 2017, eBay in 2014, Equifax in 2017, Yahoo in 2013 and 2014, Uber in 2016, Under Armour in 2018, LinkedIn in 2012 and 2021, Facebook in 2019, Marriott in 2018, SolarWinds in 2020 and others as being the victims of data breaches, phishing scams, ransomware attacks, distributed denial of service (DDoS) attacks and other forms of cyberattack.

Despite the attention-grabbing headlines, small businesses are the preferred target for cyberattacks by hackers and bad actors.

Small Business Cyberattack Risk by the Numbers

1 IN 5

Every five years, 20 percent of small and medium-sized businesses suffer from data loss due to a significant disaster.

60%

According to Datto, ransomware remains the most common cyberthreat to SMBs, with 60 percent of MSPs reporting their clients attacked as of Q3 2020.

3 IN 4

In 2019, three in four SMBs in the U.S. had reported a digital attack in the preceding year, according to the Ponemon Institute.

43%

According to Accenture’s Cybercrime study, 43 percent of all cyberattacks are on small businesses.

14%

According to Accenture’s Cybercrime study, only 14 percent of SMBs are prepared to face cyberattacks.

$826 TO $653,587

SMBs spend, on average, $826 to $653,587 on cybersecurity incidents, according to Verizon’s 2021 SMB Data Breach Statistics.

95%

According to the World Economic Forum, 95 percent of cybersecurity breaches are attributed to human error.

$10.5 TRILLION

Cybercrime is estimated to increase by 15 percent, with costs reaching $10.5 trillion by 2025.

6 Small Business Cyberattacks You Haven't Heard Of

1 Efficient Escrow

ATTACK TYPE: Trojan Horse Malware

ATTACK SUMMARY: Cybercriminals stole $1.5 million from California-based Efficient Escrow using a Trojan horse. The hackers wired three separate payments, the first $425,215 to an account in Moscow, Russia and the second and third payments totaled $1.1 million to banks in Heilongjiang Province in China. Efficient Escrow recovered the first $425,215 transaction but not the other payments. Banks are under no obligation to recoup losses from a cyberattack on commercial accounts, and unable to replace funds, were shut down by state regulators three days after reporting the loss.

2 Wrights Hotels

ATTACK TYPE: Funds Transfer Fraud

ATTACK SUMMARY: Hackers accessed the email account of Stuart Rolfe, the owner of Seattle-based Wright Hotels, a real estate investment and development firm. Once bad actors accessed his email, they could see email history with his bookkeeper and his calendar, enabling them to determine when Rolfe was busy and wouldn't check email. They impersonated Rolfe via email, directing the bookkeeper to wire money to hacker accounts in China, committing wire fraud of $1 million. After scheduling transactions, each email confirmation was deleted to not be detected immediately.

3 PATCO Construction

ATTACK TYPE: Trojan Horse Malware

ATTACK SUMMARY: Cyberthieves uploaded a Trojan horse malware program to one of the systems of Maine-based PATCO Construction, a construction firm. The hackers were able to source PATCO's online banking credentials and conduct several ACH transfers from PATCO's accounts to their own accounts. In just seven days, over $588,000 was taken from the firm. PATCO's bank was able to reclaim some of the funds, cutting the loss to $345,445. Unfortunately, PATCO had to pay interest on overdraft loans of hundreds of thousands of dollars from the bank.

4 Volunteer Voyages

ATTACK TYPE: Data Collection & Exfiltration

ATTACK SUMMARY: Cybercriminals stole the debit card number for Oregon-based Volunteer Voyages, a small business offering humanitarian volunteer trips. The attack occurred while the owner, Dr. David Krier, had just returned from a trip and was informed his account was overdrawn. The hackers stole $14,000 from his account. Since he had a business account, Krier's bank was under no obligation to reimburse him.

5 Green Ford Sales

ATTACK TYPE: Trojan Horse Malware

ATTACK SUMMARY: Criminals breached the network of Kansas-based Green Ford Sales, a car dealership. They impersonated a payroll confirmation email from First Bank Kansas to the dealership. Green Ford Sales' controller confirmed transaction details in the fake phishing email, infecting his computer with a Zeus Trojan horse. The hackers obtained the dealership's bank account information and added nine fake employees to the payroll. In 24 hours, the hackers paid the fraudulent accounts $63,000 before breach detection. With access to his computer, they intercepted confirmation emails from the bank, so the controller was unaware of the transactions in real-time. Only $41,000 in transfers could be canceled.

6 Kentucky-based Manufacturer

ATTACK TYPE: Ransomware

ATTACK SUMMARY: The network of a Kentucky-based manufacturing company was hit by ransomware, locking down each employee's computer. The CFO for the manufacturer spoke with their insurance company and IT team to determine the documents and systems the hackers had and the next steps. No proprietary information was stolen; however, the locked devices resulted in a work stoppage. Working with insurance, the manufacturer learned this hacker group would release device control based on past hacks if the ransom was paid. The manufacturer negotiated from $400,000 down to $150,000.

TPx is Your One-Stop Shop for Managed Security Services

Don't wait until it's too late. Protect your business from the growing threats of ransomware and phishing attacks with our comprehensive cybersecurity solutions.

- ✓ **Endpoint Management & Security**
  TPx protects endpoints with patch management, next-gen antivirus, remote monitoring and management (RMM), managed detection and response (MDR) and more.

- ✓ **DNS Protection**
  TPx DNS Protection enables your business to safeguard any device that accesses the Internet by blocking known malicious threats.

- ✓ **Firewall**
  TPx offers next-gen firewall (NGFW) with unified threat management (UTM), virtual private network (VPN) and managed detection and response (MDR).

- ✓ **Security Advisory Services**
  TPx advisory services provide comprehensive security consulting that can help improve your security posture and protect your business.

- ✓ **Virtual Compliance Officer (VCO)**
  TPx's Virtual Compliance Officer (VCO) service offers specialized support to design, implement and manage the information security program and controls required under applicable regulatory frameworks.

- ✓ **Cloud-to-Cloud Backup**
  TPx's Cloud-to-Cloud Backup solution provides a one-click restore for Microsoft 365 (Exchange, OneDrive, SharePoint, Groups and Teams).

- ✓ **Hybrid Backup**
  TPx's hybrid backup solution protects your data through on-premises backup with replication to secure cloud backup for redundancy.

- ✓ **Inbox Detection & Response**
  TPx's Microsoft 365 plug-in enables users to validate emails' authenticity with one click.

- ✓ **Incident Response Plan**
  TPx experts create a plan outlining how your organization should respond to and manage cybersecurity incidents.

- ✓ **Ransomware Assessment**
  TPx experts provide an in-depth review of your company's readiness to respond to a ransomware attack.

- ✓ **Security Awareness Training**
  TPx provides regular training courses with phishing simulations, following NIST guidelines.

- ✓ **Penetration Scan**
  TPx experts show how exploiting a vulnerability could result in a significant impact on your environment.

- ✓ **Vulnerability Scan**
  TPx evaluates devices connected to the network to identify vulnerabilities present due to open ports, missing patches, etc.

- ✓ **Network Security Assessment**
  TPx evaluates your organization's network security posture and profile.

- ✓ **Wireless Security Assessment**
  TPx evaluates your organization's wireless infrastructure and configuration, security posture and functional capabilities.

Why TPx for Cybersecurity?

You have enough business challenges without worrying about keeping your small business secure. Partnering with TPx provides the support it needs so you can focus on core business goals. At TPx, we have the products, services, experience and certifications to keep your network and applications secure and running safely.

Our mission is to be the easiest MSP to do business with

We solve the biggest IT issues – cybersecurity, connectivity, and collaboration – under one umbrella

We have 120+ certifications across 60+ competencies, like CompTIA, Cisco, Fortinet, Microsoft, SMC and more

We offer HIPAA, PCI DSS and SOC 2-compliant solutions

We provide enterprise-class, 24/7 support

We offer different service levels and highly customizable solutions

We have a national footprint with multi-site, multi-carrier, partner coverage

With thousands of customers nationwide, we're big enough to get the job done and small enough to be agile

We have various dedicated teams to ensure service excellence

We continuously invest in automation, self-service innovation, and back-office transformation

We are committed to providing the most densely monitored service delivery platform in the industry

We understand and embrace the criticality of our customers' performance analytics

Ready to Secure Your Business?

Contact TPx today.
Visit **https://www.tpx.com/contact-sales/** or call **866.706.7441**