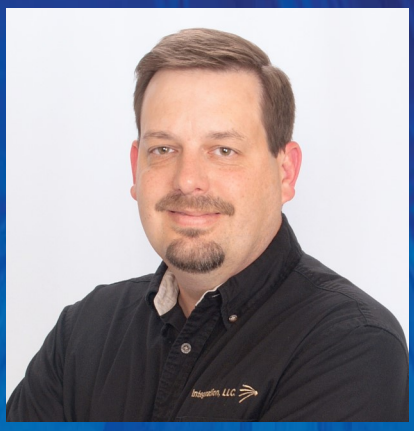
Integration Technology Times

"Insider Tips To Make Your Business Run Faster, Easier, And More Profitably"

ISSUE 3 ■ VOLUME 10 ■ MARCH 2019

What's New



This monthly newsletter is provided courtesy of Kevin Bowling, CEO of Integration.

"As a business owner, I know you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"

Loss of 1,700 Servers and 24,000 Laptops due to NotPetya Ransomware Attack

NotPetya infected computers across more than 100 countries over the course of a few days. The malware disguised itself as the Petya ransomware to gain administrator access to thousands of computers globally.

In addition to Mondelez, NotPetya affected a variety of global organizations, including:

FedEx: Global courier delivery services company FedEx estimated that NotPetya resulted in $300 million in lost business and cleanup costs.

Beiersdorf: Beiersdorf, a German consumer products provider, suffered a financial loss in the first half of 2017 due to shipping and production delays caused by NotPetya computer and system outages.

Maersk: Container shipping company Maersk has attributed at least $300 million in financial losses to NotPetya.

NotPetya has cost organizations at least $1.2 billion in combined quarterly and yearly revenue, endpoint detection and response (EDR) provider Cybereason indicated. Furthermore, cyber risk analytics platform company Cyence has estimated that insurance companies would need to pay $81.7 billion to cover the total costs of claims related to NotPetya and other cyberattacks.

Mondelez International lost 1,700 servers and 24,000 laptops due to NotPetya, *The Register* reported.

NotPetya was "the most destructive and costly cyberattack in history," according to the White House. It was launched as part of the Kremlin's effort to destabilize Ukraine.

So ask yourself: How well is my business covered?

Why Your Business Is The PERFECT Target For Hackers Is Your Protection Up To Date?

People never think it'll happen to them. Sure, they see the reports – 50 million-plus bundles of user data compromised by a Facebook breach; the billing information of more than 2 million T-Mobile users hacked by a mysterious malicious entity – but companies like those are massive, monolithic entities in American commerce. They're decidedly big fish, not like you and your small business. According to a recent JLT-Harvard Business Analytic Services survey, more than half of small business owners remain locked into this line of magical thinking, blissfully unaware of the threat cyber crime poses to the health of their organization.

We hate to burst the bubble of the happy-go-lucky majority, but the reality is that this optimistic attitude just does not square with the statistics. The incidents may not make the news, but small businesses are being targeted – and breached – by hackers at an astounding rate. In fact, the National Cyber Security Alliance reports that close to half of small businesses have experienced a cyber-attack and that 60 percent of the companies that succumb to one of these attacks folds completely within six months. They state that instead of zeroing in on Fortune 500 corporations, hackers actually prefer to swoop in on the little guy, with 70 percent of cybercriminals specifically targeting small businesses.

Yet according to a Paychex survey, 68 percent of small business leaders aren't worried about cyber security despite data from Hiscox indicating that more than seven out of ten small businesses are woefully unprepared for a breach.

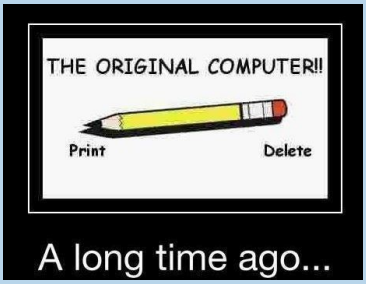
Of course, it's understandable that the average small business owner shirks their cyber security responsibilities. It's the kind of problem that's so complicated that it's tempting to sweep it under the rug. As breach tactics become more sophisticated, so do the softwares and methodologies designed to keep out criminals. In a world far removed from the days when buying a product and installing it into your network was enough, it's easy to become overwhelmed by the complexity and breakneck pace of advancing cyber security best practices. Our biases make the possibility of a hack seem remote, while our limited resources make the cost of protection appear too high to even consider.

The first step to getting savvy in 2019 is to accept that cyber-attack isn't some unlikely crisis, but a virtual inevitability. It's a tough pill to swallow, but leaving it to chance is like flipping a coin where a "tails" outcome results in your business shuttering for good.

Luckily, though an attempted hack is almost guaranteed, there are dozens of steps you can take to prevent it from doing any damage. Chief among these should be to find a managed service provider (MSP) with a long background in protecting against hacker threats to take the reins on

Continued on Page 3 ...

Funny or Brainy Quotes and Jokes



"To err is human, but to really foul things up you need a computer."

Paul R. Ehrlich

"A computer once beat me at chess, but it was no match for me at kick boxing."

Emo Philips

"The good news about computers is that they do what you tell them to do. The bad news is that they do what you tell them to do."

Ted Nelson

"One of the most feared expressions in modern times is 'The computer is down."

Norman Ralph Augustine

your cyber security as quickly as you can. It's important when auditing your internal security measures that you regularly get an outside opinion from a trusted source, in order to cover all your bases. Your internal IT departments assurances that "they've got it covered" are certainly reassuring, but to truly patch all the holes in your security barriers, you'll need more eyes on the problem. You might imagine that such a partnership must be prohibitively expensive, but they're typically more reasonable than you might think. Not to mention that when the very survival of your business is on the line, it just makes sense to budget accordingly.

The statistics paint a picture of small business owners as underprepared, unaware, and disturbingly vulnerable to the whims of cybercriminals hiding just out of view. Don't be another one of the millions of small business owners forced to shell out thousands as a consequence of wishful thinking. Wake up to the dangers of 2019, arm yourself against them, and secure the future of the business you've worked so hard to build.

3 Ways To Protect Your Business From Cyber-Attacks

1. Plan for the worst.
The sad truth is that, no matter how much most businesses prepare their defenses for a cyber-attack, a breach will often occur anyway. That doesn't mean you shouldn't invest in protection, but you should always have a plan in place if and when crisis strikes. Include actions to contain the breach, patch the affected systems, and coordinate teams (not just IT) to stay on top of the problem.

2. Keep your team in the know.
The vast majority of breaches are instigated through minor errors by everyday employees. These noncompliant security behaviors aren't just bad for your business; they're bad for PR. That's why cyber security should be everyone's priority, not just the techies in your business. That means educating everyone on what to watch out for and what to do when hackers come knocking at your door.

3. Budget for robust cyber security.
Of course, all of these measures won't mean a thing if you don't actually invest in cyber security. Instead of a one-and-done task to check off, cyber security actions should be a regular component of your day-today. Include the costs of training, employee time, documentation, consulting and the latest security innovations.

Best way to know, contact us today, we will perform an audit to give you peace of mind.

Computer Service

- ⇒ Pro-Active Customer Care
- ⇒ Onsite Computer Service/Support
- ⇒ Network Management/Support
- ⇒ Network & Server Installations
- ⇒ Network Security & Firewalls
- ⇒ Cloud Solutions & Hosted Email
- ⇒ Secure Remote Access / VPNs

Healthcare Services Provided

- ⇒ Medical, Dental, Radiology
- ⇒ Software & Hardware Integration
- ⇒ Security Solutions

Backup & Disaster Recovery

- ⇒ Business Continuity
- ⇒ Secure & Compliant Offsite Backup
- ⇒ HiTech BDR

Specialize in DFAR planning

Email, Web & Archiving

- ⇒ Spam Filtering
- ⇒ Email Hosting
- ⇒ Email Encryption & Archiving
- ⇒ Website Hosting
- ⇒ Customer Hosting Server

VOIP (Hosted)

Ask us about—Managed Services

How would you like to pay a flat rate and have us take 100% responsibility?

How would you like new equipment, service and support for a flat rate and refresh every 3 years?

Integration

Po Box 5526
Decatur, AL 35601
Phone: 256.536.5805

How would you like the security of knowing that your data is safe and protected?

How would you like a VOIP phone system that is cost effective, saves you money, and you can take it home or vacation and work as in the office?