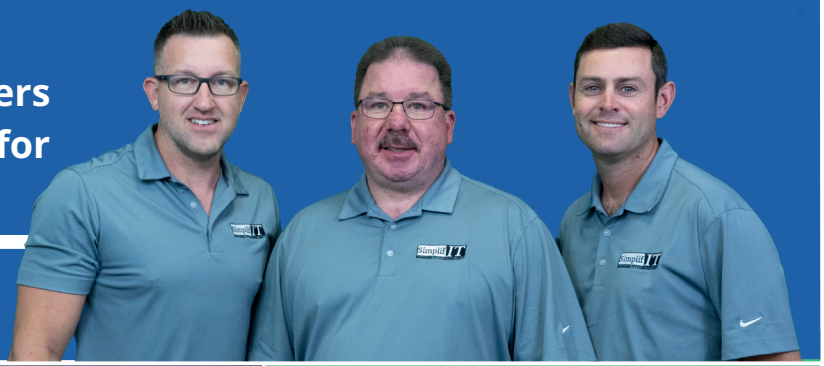
The SimplifIT Advantage

Proven strategies to help leaders make clear technology decisions for measureable business results.



Business leaders depend on technology. SimplifIT allows you to focus on growing your business with secure and compliant IT solutions that are proven to work & keep you safe.

- Craig Willard, COO
- Eric Elder, CTO
- Nick Landers, CMO

SimplifIT
MANAGED IT | CYBERSECURITY

A Message From Our Team

This month, we want to address something that affects every business leader who depends on vendors to store, manage, or transmit data: the reality that vendor breaches are no longer rare events.

In May 2026, Canvas LMS suffered what is now recognized as the largest educational data breach in history. 275 million records. 8,800 institutions affected. All eight Ivy League universities compromised. The company paid a ransom. Whether the data was actually destroyed remains an open question.

If your business relies on trusted vendors for critical operations, this breach offers lessons that apply directly to you. The question isn't whether your vendors could be breached. The question is whether you'll be ready when they are.

We are also addressing a question we hear often from business leaders: what should a strong incident response plan actually look like? Not as a technical document, but as a practical tool you can execute when something goes wrong. If your plan hasn't been tested or doesn't include clear guidance on AI risks and IT policies, this issue gives you a framework to build one that works.

This month covers vendor risk, incident response planning in plain English, and what your team needs to know before the next breach happens.

We hope it is useful. As always, we are here when you need us.

All the best!

The Team at SimplifIT

Inside This Issue

The Canvas Breach Explained: What Business Leaders Need to Know

Between May 1st and May 11th, 2026, a hacking group called ShinyHunters compromised one of the largest educational technology platforms in the world. Canvas LMS, owned by Instructure and used by more than 8,800 educational institutions across 50 countries, suffered what is now recognized as the largest educational data breach in history.

The result: approximately 275 million records stolen, representing roughly 3.65 terabytes of data. All eight Ivy League universities were affected, along with major state schools, community colleges, and K-12 districts across the United States. Instructure paid an undisclosed ransom in an attempt to have the stolen data destroyed. Whether that actually happened remains an open question.

If your business doesn't operate in education, this might feel like someone else's problem. It isn't. The lessons from Canvas apply directly to any business that depends on a trusted vendor to store, manage, or transmit sensitive information.

What Actually Happened

ShinyHunters gained unauthorized access to Canvas systems during finals week. The timing wasn't accidental. When systems are under the most stress and users are the most distracted, attackers have the best opportunity to operate undetected.

Over the course of 11 days, attackers extracted massive volumes of data while institutions continued operating as normal. Most didn't know anything had happened until Instructure began notifying affected organizations weeks later.

What Data Was Breached

The compromised data included names, institutional email addresses, student ID numbers, and private messages exchanged between students, teachers, and advisors. That means personal conversations about academic struggles, medical accommodation requests, and advisor communications are now in the hands of criminals.

Passwords, Social Security numbers, birth dates, and financial information were not part of the breach. Canvas does not store that type of data in the systems that were compromised. That limitation matters, but it doesn't eliminate the risk.

The real danger isn't the data itself. It's what attackers can do with it.

Why This Matters for Business Leaders

The Canvas breach offers several lessons that every business leader should internalize, regardless of industry.

First, trusted vendors are not immune. Canvas is a market leader. Instructure is a publicly traded company with resources, certifications, and a reputation built over years. None of that prevented the breach.

If you operate under the assumption that your vendors are secure simply because they're established or well-known, this is a reminder to verify that assumption regularly.

Second, timing matters. Attackers understand operational pressure and exploit it. For a business, that might mean targeting you during tax season, year-end close, or a product launch. When you're under the most stress, you're the most vulnerable.

Third, the breach itself is only the beginning. The stolen data creates a foundation for follow-on attacks that will unfold over months and years. With real names, real relationships, and real context, attackers can craft highly targeted spear-phishing campaigns and impersonate trusted contacts in scenarios that are nearly impossible to detect without training and verification processes.

A student who had private messages exposed is now vulnerable to someone impersonating their advisor. The data gives attackers the ability to manufacture trust, and trust is the foundation of nearly every successful cyberattack.

Fourth, centralized systems create centralized risk. Canvas serves millions of users through a single platform. One compromise affected institutions across the globe simultaneously. If your business depends on a centralized vendor for customer data, financial records, or operational systems, you are operating with the same structural risk.

Fifth, ransomware pays. Instructure paid the ransom. That decision validates the attacker's business model. ShinyHunters was rewarded. Other groups are watching. The more ransomware proves to be profitable, the more attacks will follow.

The Lesson You Can Act On

You cannot eliminate vendor risk. But you can manage it.

That means knowing which vendors have access to your data, what data they hold, and what their breach notification process looks like. It means having contract language that defines expectations around security and incident response. It means reviewing vendor security posture regularly, not just during onboarding.

It also means preparing your organization for the reality that a breach will eventually happen. When it does, your response speed and ability to contain the damage will determine the outcome.

The Canvas breach happened to a well-resourced organization that millions of users trusted. That reality should be sobering for every business leader.

The question isn't whether your vendors could be breached. The question is whether you'll be ready when they are.

Team Spotlight: Eric Elder
SimplifIT CTO

Every once in a while, you get to work with someone whose expertise runs deep enough that complex problems become simple conversations. That's Eric Elder, SimplifIT's Chief Technology Officer and founding partner. Eric brings over 20 years of IT experience, much of it spent solving problems where getting it wrong wasn't an option. He served as IT Director for a $2 billion publicly traded multi-site community bank, managing technology under federal and state regulatory oversight. That background shaped how he approaches IT strategy today: with the discipline of someone who knows what compliance actually requires, the technical depth to engineer solutions that work under pressure, and the clarity to explain complex environments in ways business leaders can act on.

Eric's compliance expertise runs deep. He brings years of experience navigating federal and state level compliance frameworks like GLBA, SOX, and FFIEC. For SimplifIT clients in highly regulated industries like accounting, legal, DoD contracting, and financial services, that background translates directly into faster implementations, cleaner documentation, and less risk. His technical accomplishments aren't theoretical either. He successfully migrated 75+ physical servers into a virtualized environment for decreased total cost of ownership and five 9's reliability. But what matters most to business leaders is that Eric's technical expertise exists to solve business problems, not to create them.

What stands out most is Eric's ability to take a complex, tangled IT environment and make it simple, standardized, and manageable. He's passionate about changing the mindset toward IT from being a cost center to being an integral part of profitability. Ready to discuss your IT strategy? Contact Eric Elder at Eric@WeSimplifIT.com or call 502.783.6630.

What a Good Incident Response Plan Looks Like (In Plain English)

Most businesses don't have an incident response plan. The ones that do often have a document that's never been tested, rarely understood, and impossible to execute when something goes wrong. A good incident response plan isn't a technical document. It's a business continuity tool written for the people who will make decisions under pressure. Here's what that looks like.

It Starts Before the Incident

A strong plan begins with clarity about what you're protecting and who's responsible. That means knowing where your critical data lives, who has access, and what your obligations are if it gets compromised. It means documenting vendors, cloud services, backup systems, and communication channels.

Most importantly, it means having current contact information for everyone who will need to act: internal leadership, your IT provider, cyber insurance carrier, legal counsel, and any incident response firm you've identified. If that information is outdated or incomplete, your plan isn't ready.

Detection and Reporting

Your plan should make it easy for your team to recognize when something is wrong and know exactly who to contact. Include clear examples: ransomware, unauthorized access, suspected breach, phishing compromise, lost devices, vendor breach notification. The rule should be simple: when in doubt, report it.

Containment

Once an incident is confirmed, the priority is stopping it from spreading. That means isolating affected systems, disabling compromised accounts, and preventing further damage.

Your plan should document who has authority to make containment decisions. Can you take a server offline? Who decides whether to shut down email or disable remote access? These are not decisions you want to figure out in real time.

Assessment and Communication

You need to understand what happened, what data was affected, and who needs to be notified. Your plan should outline how to preserve evidence, assess the scope, and meet notification obligations.

Internal communication matters too. Who tells the team what's happening? What gets communicated to clients? A good plan includes draft templates so you're not writing from scratch under pressure.

Recovery

Your plan should document recovery priorities: what gets restored first, how backups are validated, and what security measures get implemented. After recovery, conduct a post-incident review. What worked? What didn't?

The Missing Piece: IT and Cybersecurity Policies

Here's what most plans overlook: clear IT and cybersecurity policies prevent incidents before they happen. Your incident response plan and your IT policies should work together. If your team doesn't know what's allowed, you're creating risk before an attacker shows up.

AI Acceptable Use Policy: The Gap Most Businesses Still Have

Most businesses still don't have an AI acceptable use policy, and that gap is a real vulnerability. Employees are already using AI tools: ChatGPT, meeting transcription services, browser extensions. The question isn't whether your team is using AI. It's whether they're using it safely.

A strong AI policy defines which tools are approved, what data cannot be shared with AI systems, and consequences for violating those rules. Unapproved tools create security and compliance risk, especially if sensitive data ends up in third-party systems you don't control.

Your incident response plan should address what happens when an AI tool is compromised or when an employee shares restricted data through an unapproved platform.

The same applies to every IT policy: passwords, multi-factor authentication, acceptable use, remote access, BYOD, vendor security, and data handling. If your policies aren't documented and your team hasn't been trained, your incident response plan is fixing problems that clear policies could have prevented.

Test It Before You Need It

Run a tabletop exercise with your leadership team. Walk through a realistic scenario and see where the plan breaks down. You'll find gaps in contact information, unclear decision authority, and assumptions that don't hold under pressure.

Fix those gaps now, not during an actual breach.

The Bottom Line

A good incident response plan is clear, tested, and designed for the people who will use it. It starts with strong policies that prevent incidents and includes a defined process for handling them when they happen.

If your plan hasn't been reviewed in 12 months, it's outdated. If it's never been tested, you don't know whether it works. The best time to build your plan was before your last close call. The second-best time is today.

AI Profit & Efficiency Assessment: Let's Identify Real AI Opportunities That Drive Business Results

Here's what we know: the businesses winning with AI aren't chasing hype. They're finding practical opportunities to save time, reduce costs, and improve efficiency. That's exactly what this assessment is designed to uncover.

What We'll Cover:

- Identify practical AI opportunities within your business - Discover repetitive tasks and operational bottlenecks
- Evaluate current AI usage and potential security risks - Receive an Executive AI Opportunity Scorecard
- Get a Crawl → Walk → Run AI roadmap - Designed to deliver practical business outcomes—not AI hype

Scan The QR Code To Schedule Your AI Assessment Today

Simplif IT
MANAGED IT | CYBERSECURITY

102 Enterprise Drive
Suite A
Frankfort, KY 40601

502.783.6630

WeSimplifIT.com

Why Small Businesses Are Still Stuck with AI (And Where to Start)

Most small businesses know they should be doing something with AI. They're just not sure what that something is.

The problem isn't lack of interest. It's the overwhelming number of options, the fear of picking the wrong tool, and the pressure to "do AI" without a clear plan for what success looks like. Here's what we're seeing: businesses start with the tool instead of the problem. They sign up for the latest AI platform, spend weeks trying to fit it into their workflow, and end up with another unused subscription and a more skeptical team.

Start With the Outcome, Not the Tool

The businesses getting real results from AI aren't asking "What AI tool should we buy?" They're asking "What problem are we trying to solve?" Reduce email response time. Automate repetitive reporting. Improve meeting follow-up. Those are outcomes. Once you're clear on the outcome, the tool becomes obvious.

The Crawl, Walk, Run Process

The right way to adopt AI is the same way you'd adopt any business change: start small, build confidence, and scale what works.

Crawl: Pick your biggest bottleneck. Choose one process to pilot. Use simple, low-risk tools like AI-powered email responses or meeting summaries.

Walk: Measure the results. Train your team on what works. Expand to two or three use cases like scheduling automation or reporting assistance.

Run: Deploy across departments. Integrate into daily workflows. Build custom solutions as needed.

The Bottom Line

Don't let the AI hype freeze you. Start small. Focus on measurable outcomes. Build momentum. The businesses winning with AI didn't start with a massive rollout. They started with one smart, targeted use case.

CYBER INSURANCE READINESS CHECKLIST

Is your cyber insurance renewing soon?

Whether you are just looking to check a box, ensure that you can get coverage for cyber liability insurance, or improve the security of your organization, this checklist will help you prepare.

Check each common requirement and rate your readiness:

- ☐ Email security is enabled in your email system (DKIM, DMARC, SPF)
- ☐ DNS filtering or web filtering is in place to block malicious web content
- ☐ Advanced Anti-malware/spyware/ransomware software is deployed on all systems
- ☐ User installed programs are limited to only pre-approved applications
- ☐ User training is in place to educate against threats like phishing and ransomware weekly or monthly
- ☐ Perimeter traffic is monitored
- ☐ Internal network traffic is monitored
- ☐ Multi-factor authentication is in place for users
- ☐ All Systems are backed up daily to an offsite or cloud location with the ability to restore
- ☐ Disaster recovery and incident response plans are in place, reviewed and tested annually
- ☐ All available important and critical patches are installed within 7 business days across systems and software
- ☐ Managed Detection and Response (MDR) is installed on all computers and servers

Rate your Cyber Insurance Readiness: ____ / 12

If you need to address any of these requirements, contact us now to start planning for your next renewal. We suggest reviewing this list before you submit your application.

Do you know another business we can serve? Ask us about our referral program.