YOU'RE EVEN MORE VULNERABLE THAN YOU THINK...

Let Rusty Gilmore show you where
your weakness lies—before it's too late.

PLAN. PROTECT. PROSPER.

Introducing Russell "Rusty" Gilmore, *EnCE, CISM, CISSP*

Security Consultant and Computer Forensic Expert

Long before his days as a security consultant and computer forensic expert at Protus3, Rusty Gilmore sought to protect and serve the people of North Carolina as an officer with the Raleigh Police Department. His tenacity for discovering leads and using deductive logic took him from beat cop to detective… with a stint on the Federal Drug Task Force along the way. But not all his days were spent analyzing fingerprints and questioning high-profile suspects. "When I was a police officer," Rusty said, "I would sometimes have to sift through garbage to find evidence. It wasn't always as glamorous as you see on TV."

Now, with Protus3, Rusty applies this same in-depth analysis and sleuthing while confronting breaches in computers and other electronic devices. At the same time, he counsels his clients to be proactive in protecting their data.

Rusty's progression from police detective to computer forensic expert was actually rather organic. His father had worked for IBM, and "since childhood, computers were part of my life as long as I can remember," he said. "I took them apart and put them back together and always had the desire to tinker with them." After about nine years with the Raleigh Police Department, he decided to open his own computer business. He did repairs and network upgrades before starting work for the federal government as an IT security contractor.

Throughout his career, Rusty has consulted on several high-profile and nationally recognized computer and technology misappropriation cases. He's dealt with data theft, deletion of data, murder cases, hacking cases, wire fraud investigations, and quite a few domestic cases. As an expert, he is highly sought after by attorneys and even consulted with both sides on a local high-profile case. He has also worked with the FBI.

Rusty has a B.S. in Information Technology & Security from Campbell University and an Associate's Degree in Criminal Justice from Wake Technical Community College. Rusty is a Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), and a EnCase Certified Examiner (EnCE).

> **"I may have searched through people's garbage as a police officer," he said, "but you learn a whole lot more looking at their computers."**

But what really makes Rusty an expert goes beyond his keen ability to make sense of data and keep up with the latest computer technology. "It's complicated," he said, "but whether it's a criminal or civil case, I work to understand what my client is looking for—and I look at the data and provide them with the information they need to move forward."

Computer forensics has universal relevance and applications. Rusty has given presentations, trainings, and consulting advice to a wide variety of industries, and he would welcome the opportunity to share his expertise and experience. He can speak on a broad spectrum of topics to anyone with a technology-related stake in an entity or who might be at risk of sticky HR situations, malware, employee malfeasance, or other data breaches.

His audiences include:

- Biotechnology startups
- Small practice doctors and attorneys
- Pharmaceutical companies
- Food and beverage manufacturers
- Schools and universities
- Foundations and nonprofits
- Real estate agents
- Insurance agents
- Business leaders
- Chambers of commerce
- Developers
- Churches

Sample topics include:

1 Preventive Steps Every Business Should Take

The first line of defense to computer security breaches is to have a good defense. Limiting access to sensitive files, rotating passwords, spyware, virus detection and employee training are some simple steps every business can make to improve their computer system security. The first question in every investigation of a security breach is often: What security measures were in place to begin with? Being proactive, consistent and informed can make a difference in stopping cybersecurity breaches, theft and misappropriation.

2 Proper Training Can Mean The Difference Between Success And Failure

Installing the proper computer firewalls and security system is useless without people to actually do the work. The buck doesn't stop at the installation of hardware or software. The fact remains that the single greatest risk for companies are their own employees (whether by clicking on malware or conducting deliberate espionage or theft). What if that employee hadn't opened the attachment? What if your IT department had installed the latest firewall protection? What if there was an alarm on vital files to prevent theft? Training a company's employees to identify risks is key to having a successful integrated security system. While accidents do happen, the goal is to limit those chances and limit the possibility of Murphy's Law ruining your business.

3 Policing The Police | Never Hand Over All The Keys

Most companies usually have an IT professional (or department) that is responsible for all the computer systems of the company. The mistake is made when one or two people are the only individuals who know exactly how your network operates. Who can you call when the person with all the passwords is the one suspected of malfeasance? If they know how they operate, they will know how to work around them. This is timely advice for companies on the best practices to supervise and safeguard against cybersecurity breaches and theft by your own employee.

4 Storage. Backups. Cleansing.

How often should you back up your files? Where should the information be stored? Can you erase the data off the computer? Should you really hit the reset button? These issues are faced by many companies, especially with instances of unexpected employee turnover and transition. Having a plan in place well before you find yourself scrambling around trying to locate old files, data and emails will save time, resources and headaches in the future.

5 I've Been Breached...Now What?

In the movies, a security breach is indicated by a menacing skull and bones on every computer screen in a company. In reality, many breaches are discovered one of two ways: either immediately (because you are suddenly locked out of your system) or at some later time, when you discover a file is missing or corrupted. The steps you take immediately after a breach can mean the difference between closing the caper and having your case go into the unsolved mystery file. Turning off your computer might not be the best solution in certain circumstances. Having a plan in place before anyone takes additional steps is vital in cybercrime investigations.

6 (WECID) What Else Can I Do?

Cybercrimes do not always involve removing valuable files off an employee's desktop or the main server. In addition, payroll manipulations, credit card charges, employee records, and personal information leaks should be a concern for both companies and individuals alike. In some cases, the employer has a fiduciary duty to protect and secure private and sensitive information. The lawyers handle the legal ramifications. Rusty just tells you how to best defend yourself and your interests.