



MAY/JUNE 2011 • VOLUME 4 • ISSUE 3

US Edition 



**info security**

www.infosecurity-us.com

STRATEGY.INSIGHT.TECHNIQUE.

# Charting Your Course

**How to Navigate A Successful Infosec Career**

**Plus:**

**Spotlight on Education & Careers**

**Inside the Mind of Bruce Schneier**

**Springtime Flooded by Data Breaches**

# R&D



Lauren Moraski



**[The security] industry is largely built on a bunch of alarm systems that say your house got broken into a week ago**

David Koretz

# All Eyes on *CSI: Cyberspace*

In an ever-changing world, the way crimes are committed, and subsequently investigated, must also change. **Lauren Moraski** takes us inside the world of modern-day cybercrime forensic investigation

This is the internet: an evolving tool of commerce, a galaxy of information and a revolutionary social environment connecting the world. But there are some who abuse this technological advancement to exploit and steal from innocent citizens and businesses. It's my job to stop them. My partner is my laptop. The captain is the chief information security officer. I'm an IT forensic expert.

If there were a *Dagnet* episode about cybercrime, then you might imagine the opening narration would sound something like this. In reality, the essence of investigating fraudulent online activity doesn't stray too far from examining any other crime – although the tools are much different. An informal survey of experts suggests that forensic tools are not only more ubiquitous, but they're both improving and getting easier to use in this age of "CSI: Cyberspace".

## "Just the Facts Ma'am"

With most cybercrimes executed across borders, we no longer rely as heavily on such *Dagnet*-era fact gathering tools as interviews or video surveillance to build a case. Digital evidence is considered "intrinsically important", says James Harris, acting unit chief of Cybercrime Unit 2 at the FBI.

With a cybercrime, everything leaves a trail. "Almost every crime committed today

involves some degree of electronic evidence", adds Mark Rasche, director of cybersecurity at CSC, a cybersecurity firm based in Falls Church, Virginia.

"Forensics isn't just recovering deleted files", notes Rob Lee, the curriculum lead for digital forensic training at the SANS Institute. "It's more the analysis of digital artifacts to be able to tell a factually based story of what a human created."

Frank Coggrave, general manager EMEA of Guidance Software, says the data collected during his team's investigations have made it "all the way to the [US] Supreme Court".

Some say that with web applications, for example, early detection and response are key components to any cybercrime. David Koretz, founder of Mykonos Software, a web application security company, says: "Forensics is great, but the first goal should be prevention."

## The Cybercrime Nitty-Gritty

No two cybercrimes are the same, and the approaches vary depending on the tools deployed and the investigators on the case. In short, according to Rasche, the steps used in IT forensics include identification, acquisition, analysis and reporting.

Laura Mather, former fraud prevention expert at eBay – who now runs SilverTail Systems – says, simply put: you need find how

the bad guy got in and how he perpetrated the crime. But that's not always easy.



**You're either able to think like a criminal or not**



Lisa Mather, SilverTail Systems



## Almost every crime committed today involves some degree of electronic evidence



Mark Rasche, CSC

"There were many attacks happening at eBay", she recalls. "It came down to trying to plug all the holes in the dam. We didn't have time to be strategic." Nevertheless, a strategic road map is necessary these days. Mather says that examining a cybercrime is analogous to investigating a crime in the real world: you need to understand motive.

"Each situation is different", adds the FBI's Harris. "You have to gather as much information as possible without undue hardship to the company. We have to get the logs, network connections and samples of the malware." Within the FBI the first response is usually done at the field office level, and if there aren't enough resources there, then the Cyber Action Team, a group of highly-trained forensic experts, steps in.

To understand how a forensic investigation unfolds in a web-based break-in, it's helpful to consider the phases of an attack: reconnaissance, attack vector establishment, implementation, automation, and maintenance. "An attacker is looking for vulnerability, so you want to shift your detection to the reconnaissance phase", says Koretz. He argues that the

security industry is "chasing yesterday's attack and yesterday's thinking ... this industry is largely built on a bunch of alarm systems that say your house got broken into a week ago."

So what's Koretz's solution? The minute the intruder trips the wire, the forensic investigation begins. "We start to record them so we can play it back for law enforcement", says Koretz. In a lot of ways, it's not about collecting as much data as possible. "The problem is that 90% of the data is garbage", he contends.

### One Step-By-Step Approach

We asked Lee from SANS to guide us through a step-by-step investigation of a spear phishing attack – in this case, a data breach that goes undetected at a major corporation.

How does the investigation begin? In the majority of external attacks, "the adversary makes a mistake and they're detected internally, which happens about 20% to 30% of the time", says Lee. He notes that between 70% and 80% of the time, local management is contacted by law enforcement to let them know they're victims of a data breach.

In the past, the initial knee-jerk reaction was to pull all the affected systems offline. But Lee says during the first phase of the attack the key is not to react. This way, the adversary will likely not branch out and hit additional systems. "You almost have to be sitting there, staring at the bear", Lee jokes. "If you move aggressively, you can end up hurting yourself even worse."



SANS' Lee says that during the first phase of a detected cyber attack the key is to not react, which sounds like a high-stakes game of chicken

The goal is to pull the data off the systems to find out what malware was used and how it's spreading. Then it's time to start leveraging "threat intelligence" in order to prevent and detect the next attack. "You really have one shot initially of doing this correctly", Lee warns.



Frank Coggrave, Guidance Software

"Once you've identified the hosts that are compromised, we enter 'remediation weekend' and go through a set of measures in order to take all the machines down simultaneously...change all the passwords, pull the connection from the internet", he continues. "Basically it's an abrupt shove of the adversary out of the network. Then using the threat intelligence you gathered earlier, you move into a more aggressive stance. Now you know the adversary is immediately trying to get back in, so you deploy additional resources and start that additional detection."

At this time, it's crucial to have clear metrics in what will likely become an ongoing battle. Lee likens the process to gardening, explaining: "You'll never have a garden that's completely weed-free. You'll always have to remove the weeds and look for rodents."

Gathering accurate forensics can get particularly tricky when perpetrators try to cover their tracks by doing anything from

deleting files and using fake IP addresses to installing logic bombs and trip wires. Fraudsters can also conceal the origin of malware or a piece of malicious code, making it more difficult for an investigator to locate core evidence.

## The Brains Behind the Investigation

What does it take to become a successful cybercrime investigator? That depends on whom you ask. When SilverTali's Mather interviews a new candidate, she almost always asks the same question: "Tell me how you would get through an airport without a ticket." She notes, "You're either able to think like a criminal or not. I have that DNA. I can say if you want to defraud this, here's how I'd do it."

Rasche, meanwhile, thinks investigators need to have a deep knowledge of the technology. Coggrave observes that many digital forensic investigators are former members of law enforcement. "They have a good understanding of the process and can grasp the chain of evidence", he says.

There are a growing number of universities now offering master's-level courses in the subject, but cybercrime detectives can sprout from many different backgrounds. Mather says good forensic investigators tend to come out of information technology. Forensic investigators are becoming more specialized by gaining expertise in niche areas. Still, Lee laments that more experts are needed. Lee thinks large corporations should have at least one investigator for every 8,000-10,000 workstations.

## Inside the Law

As cybercrime becomes more prevalent, experts are increasingly seeing businesses working more closely with law enforcement and other government agencies. With that, the FBI – for one – has stepped up its efforts. "Within the cyber division we have a rigorous training curriculum", says Harris, who adds that an increasing number of FBI agents are becoming Certified Information Systems Security Professionals (CISSPs).

Agents on a cyber career path can be in jeopardy of losing their jobs if they don't



Joe Friday worked here, and he carried a badge. But if he were a detective today, he would also be lugging a laptop, and consulting with forensic investigators of a new breed

keep up with the training, he says. "We make those [training classes] available for our local and state departments as well, so everyone has a good grounding on these types of digital forensics", Harris notes. The FBI aims to keep up with the latest trends and tools – most recently focusing on reverse engineering of malware.

Lee believes law enforcement agencies have "so many talented people", but just not enough of them. He adds: "Technology is moving much faster than our investigators are able to keep up with. We have a tenth of the people we need trained. The same is true for corporations."

Mather is impressed by the role of government agencies, especially the US Secret Service. But, she notes, "there's always going to be less resources for these government types of initiatives." She is, however, "optimistic" about the Obama administration's "latest focus on cybersecurity". Still, no matter how much the US does to tackle cybercrime, many jurisdictional and logistical issues come into play when tracking down the perpetrator.

## Nabbing the Criminal

Once investigators gather and analyze data, the information is often handed over to law enforcement, but it's difficult to actually

track down the suspect and ultimately achieve justice. Insiders say most cases go unprosecuted because the alleged criminals are simply overseas or the legal system can't keep up with the technology. Not only is it difficult to prosecute across borders, but some companies don't report crimes because of the potential risk to reputation. Coggrave says there's a lot of "brushing under the carpet".

Still, the legal hindrances haven't deterred forensic investigators. "Forensic response teams are getting a lot better", Lee admits. And they're changing their approach. Investigators are learning that fighting a cybercrime doesn't always have a clear end point. "You go in, you fight crime and then you come home", he says. "You can't go back to a completely clean whiteboard. You're always going to be bleeding a little. It's a matter of how fast you can plug the holes."

If Dagnet's Sergeant Joe Friday were an IT forensic expert, he'd still be interested in motive, but instead of fighting criminals on the streets, he'd be doing it from behind his laptop. To serve and protect doesn't always mean flashing a badge or carrying a gun. It can be scanning internet traffic, dissecting malware and analyzing data in an effort to protect "the good citizens" of this great world – even the citizens of Los Angeles. ■