



“I’d rather have my limited IT resources focused on helping us practice law more efficiently... not spending all of their time battling spam, spyware, viruses, and cyber-crooks.”

Bruce Rosen  
Partner



#### INDUSTRY Law

##### ABSTRACT

McCusker, Anselmi, Rosen, Carvelli & Walsh, P.C. relies on the Internet for client communications and legal research among other things. Bruce Rosen is the partner in charge of the Firm’s IT services and has a skeleton staff to manage the technology needs of his 26 attorney practice. His Firm was the victim of a carefully crafted Internet attack designed to commandeer his computers as slave servers to broadcast SPAM e-mail, and redistribute pirated video. This compromise went undetected despite having firewall and anti-virus services. Before it was over, the law firm had its email blocked due to ‘blacklisting’ by several major anti-spam services, was forced to rebuild its mail servers, and spent an inordinate amount of time probing their network for a deeply rooted, undetectable gremlin. The real solution was turning to Network Box for an innovative subscription-based managed security service that provides a multi-pronged approach to thwart complex blended digital threats.

##### BACKGROUND

McCusker, Anselmi, Rosen, Carvelli & Walsh, P.C. (“MARCW”) has been in practice for ten years in Chatham, New Jersey. The Firm’s 26 attorneys have expertise ranging from First Amendment issues, to complex commercial law and real estate transactions, to white collar criminal defense and employment law matters. The firm’s clients include many high profile and Fortune 100 companies.

The Firm makes significant use of the Internet for client communications and legal research. Bruce Rosen is the Firm’s partner in charge of IT services. As he sees it, the Internet has become an “essential business service” for his Firm, and he believes “the continuity of Firm business depends on reliable, secure access to the Internet.” Like most Firms, he had a firewall installed between his network and the Internet, and his IT staff makes certain that antivirus software on their servers and desktops is up to date.

However, the Firm’s network was compromised last year by professional hackers.

All trademarks are the property of their respective owners.

This case study was authorized by McCusker, Anselmi, Rosen, Carvelli & Walsh, P.C.

Network Box LLC  
Newport Financial Center  
111 Pavonia Avenue, 4th Floor  
Jersey City, NJ, USA 07310  
Web: [www.network-box.us](http://www.network-box.us)



These digital criminals took control of their mail server and were broadcasting thousands of spam messages per hour. They had commandeered portions of the hard driver to hide stores of pirated videos. These malicious activities had forced major Internet anti-spam services to blacklist the firm's servers and IP addresses, resulting in the automatic rejection of their emails by many recipients' mail systems. Bruce had the unfortunate responsibility of asking some of the Firm's blue chip clients to please accept e-mail transactions through outside temporary addresses while the problem was rooted out. As far as Bruce was concerned, regardless of the compromise to the Firm's servers, the potential compromise to their thriving practice and emerging brand value of MARCW was even worse.

#### DISCUSSION

Bruce was sure his IT consultants had done everything necessary to keep the firm's computer network properly protected. In addition to a name-brand firewall, his firm had anti-virus software running on all their desktop machines and their email server to ensure full mailbox scanning and cleansing. There was a reasonable sense of calm before what would become a network storm. Access to the Internet and the subtle access to the Firm's daily business operation had become transparent. MARCW had become wholly dependent on the real time communication and access to a wide range of research resources.

It started simply enough. One, then two, then four or five clients started complaining to various staff at the Firm that they were not receiving expected e-mail transmissions from several of the lawyers, including Bruce. Of course, he presumed there was a glitch in their mail server and phoned their IT consultants who immediately responded. Two hours later, his IT consultant arrived in his office. Disturbing news: the

reason clients hadn't received lawyers' e-mail was that the Firm's network "domain" and IP address had been placed on several major anti-spam blacklists, so their client's email servers, which rely on these block lists to cut down on spam, were automatically rejecting transmissions coming from his firm. "Of course, we assumed there had been some sort of mistake," recalls Bruce, "but when our IT people looked deeper they found our e-mail server had been broken into, and was being controlled by spammers. We couldn't communicate with some of our largest clients and not even the courts were receiving our messages. The situation quickly became completely untenable."

It went from bad to worse. In fact, while the firm's e-mails were being rejected by their clients' servers, hackers were relaying literally hundreds of thousands of spam e-mails a day through the Firm's compromised mail server and were using hidden directories to warehouse pirated videos. Bruce's IT team was now locked in battle trying to chase down the digital gremlins, restore mail services and deal with the large, volunteer-based, and omni-present black list services such as Spamhaus.Org, while trying to call in reinforcements to track down the trouble. Their anti-virus tools providers – *one of the best known brands in the business* – never identified a problem, let alone suspicious behavior. Moreover, they were continuously running scans of their network servers and Microsoft Exchange database, turning up nothing suspicious. Ultimately, Bruce and his IT team had to call in and pay for a complete ground up rebuild of the mail server and databases by the manufacturer.

The source of the compromise was never determined. The hack remains a mystery, and it took custom code from the manufacturer to properly rebuild their Microsoft Exchange services and root out the grem-

McCusker, Anselmi,  
Rosen, Carvelli  
& Walsh, P.C.

All trademarks are the property of their respective owners.

This case study was authorized by McCusker, Anselmi, Rosen, Carvelli & Walsh, P.C.

Network Box LLC  
Newport Financial Center  
111 Pavonia Avenue, 4th Floor  
Jersey City, NJ, USA 07310  
Web: [www.network-box.us](http://www.network-box.us)



lins. Even with that done, it still took days to extricate their domain name and IP address from the Internet black lists so they could restore online communications and services to their clients and the courts.

Although the problem seemed fixed, actually Bruce had only addressed a specific incident. The root cause remained unabated. After two days rebuilding their servers and restoring Internet service, a cold reality set in for Bruce: their anti-virus software was up to date but had turned up nothing. Their firewall was properly functioning, and yet they had been seriously hacked. "We believe we had acted competently to ensure we had adequate protection," reflected Bruce, "but clearly we hadn't."

#### THE REALITY CHECK

For Bruce, MARCW, and even his IT consultants, this was a learning experience. What they came to understand was that for all their effort to provide the correct components including a firewall and anti-virus software, they missed a critical development: the nature and complexity of security threats is rapidly changing, and disparate security components cannot protect a network without coordination and correlation. They had gained an expensive appreciation for how security threats are much more complex today than even just six months ago. Bruce realized MARCW needed to step back and consider how not only to protect their computers, but to properly secure their network. The situation was clear and the facts simple enough:

1. The Internet had become essential "infrastructure" for MARCW. In other words, Internet access, mail services, the web, and other tools for legal research and practice applications that use the Internet to reach needed resources are all required. The entire Firm's staff had come to rely on it – from client communiqués, to legal research, access to the Courts, to shipping services, even ordering supplies. Like it or not, the continuity of the Firm's business operations depends on the Internet.
2. However, with the power and accessibility of the Internet come ever increasingly complex and even criminal acts against digital assets. "Based on our nightmare experience with this network hack, we were looking at investing a significant amount of IT resources in managing security unless we could find a different approach to managing the complexity, costs, and confusion of network security," Bruce forecast.
3. Security compromises are no longer individual, unique, or isolated events or threats. What once were script-kiddies are now full blown digital criminals. An approach is required that takes into account multiple conditions, changes, events, and suspicious activity and correlates these elements and coordinates an immediate, and potentially even preemptive response.
4. Computer security is not enough – it's about the network. In fact, law firm networks remain vulnerable even if the individual desktops and servers are protected with anti-virus software. Relying on such "host-based" security alone is dangerous, since they can provide protection for only certain types of threats, are updated too infrequently, and often rely on users discretion on what constitutes an attack, At the same time, threats aren't limited to computers – all things connected to the network, such as printers and scanners, can be compromised. The best defense is to block attacks before they reach individual computers or equipment at the network's "perimeter" – the boundary between the Firm and the Internet. Unfortunately, firewalls, the traditional network perimeter guardian and the first line of defense upon which



McCusker, Anselmi,  
Rosen, Carvelli  
& Walsh, P.C.

All trademarks are the property of their respective owners.

This case study was authorized by McCusker, Anselmi, Rosen, Carvelli & Walsh, P.C.

Network Box LLC  
Newport Financial Center  
111 Pavonia Avenue, 4th Floor  
Jersey City, NJ, USA 07310  
Web: [www.network-box.us](http://www.network-box.us)



MARCW relied, provide only a small (though important) subset of the security services needed to thwart potential compromises to the network's operation and digital content stored there.

5. The risk of irreparable harm to the Firm's brand, image, and reputation in the face of a compromise of its network, a compromise of client communications, or worse, a loss or exposure of client data is a clear and present danger. Even losing a day's worth of client communications, billable or not, can have damaging consequences.
6. Adequately addressing these digital threats has become an arms race and it is neither practical nor reasonable to build your own militia to battle it, or to unplug your network and expect your clients to communicate with you through a Fax machine or U.S. mail.

office building. It's that simple. Network Box is completely outsourced managed security services – there is no hardware to buy, no software to install, no certification process for IT staff, no lengthy contract commitments or costly support agreements.

As Bruce sees it, this is precisely what MARCW needed to get back to the business of practicing law in the Internet age, without worries of digital threats or intrusions. *"I'd rather have my limited IT resources focused on helping us practice law more efficiently and making it easier for our clients and us to communicate... not spending all of their time battling spam, spyware, viruses, and cyber-crooks."* The subscription-based managed service removes the headaches and overhead of selecting, buying, installing, and operating several different security components.

To deliver this, Network Box employs a rapidly emerging technology called "unified threat management" in a powerful security appliance that stands between the Internet and the MARCW network. And what makes Network Box unlike other managed service providers is that the company develops and maintains its own specialized appliances that sit on the edge of its subscribers' networks and then manages those appliances remotely. As a result, Bruce has turned over the monitoring, surveillance, and complete management of their perimeter network security to the Security Operations Centers at Network Box. *"Since bringing in Network Box, our security concerns have disappeared. We started by just using them to supply and manage our perimeter anti-virus and anti-spam defenses, but the service proved to be so smooth and effortless that we have had them take over all firewall and VPN functions as well,"* says Bruce.

#### THE NEW TECHNOLOGY

The "unified threat management" or "UTM" approach recognizes security

Armed with this new understanding, he started looking for alternatives, and that's when he discovered Network Box Corporation, a five year veteran in providing network perimeter security (that's nearly half the life of the commercial Internet). The global parent company recently established its U.S. subsidiary in late 2005, and offers a simple but powerful approach: subscription-based network security services – precisely what Bruce was looking for.

#### THE NEW APPROACH

Bruce posed the question about why network security should be any more difficult for the average business than building security. The answer is: It shouldn't. In fact, in order for the law firm to refocus its IT resources on the matters of practice automation, network security should be "plug-in and protect." Therein the new approach of Network Box: subscription-based network security services. In other words, think "ADT®" or "Brinks®" services, but set up for your computer network rather than your

McCusker, Anselmi,  
Rosen, Carvelli  
& Walsh, P.C.

All trademarks are the property of their respective owners.

This case study was authorized by McCusker, Anselmi, Rosen, Carvelli & Walsh, P.C.

Network Box LLC  
Newport Financial Center  
111 Pavonia Avenue, 4th Floor  
Jersey City, NJ, USA 07310  
Web: [www.network-box.us](http://www.network-box.us)



threats as complex multi-point attacks and there must be coordination between the various components of network security – firewall, intrusion detection, anti-virus, anti-spyware, and so on. UTM technology consolidates all of the various required tools for proper network security including your firewall, anti-virus, anti-spam, intrusion detection, intrusion prevention, and content filtering into a single security appliance. Network Box has married the capability of unified threat management technology with carrier-grade professional Internet security management, to deliver a highly cost effective service that's completely transparent.

#### THE NETWORK BOX DIFFERENCE

Bruce puts it succinctly *“I now know firsthand that the integrity and security of our network is essential to our practice. In the end, having Network Box handle our security means one thing less that I spend time worrying about.”* Bruce's law firm now has the Network Box Internet security service installed with the UTM appliance on the edge of their network. Monitored and managed by the east coast Security Operation Center, the appliance is guarding through a multi-pronged, coordinated and correlated approach. All Internet traffic is probed and scanned before it is allowed into MARCW's network. Emails are passed through 14 different anti-virus engines and 11 different anti-spam engines. Web ad-

resses are checked against a 1.7 billion URL database to prevent users from accidentally accessing dangerous sites, while traffic from the sites that users do visit are scanned continuously for malicious code such as spyware. An intrusion prevention system is integrated directly into the firewall to block hacking attempts.

Beyond the technology, however, MARCW benefits from the active monitoring and administration of their perimeter by Network Box. While Bruce and his team decide on the security policies they want enforced, they can rely on the very people who developed the technology being used to implement those policies in the most effective, efficient and secure manner possible.

Security threats depend on the exploitation of flaws in systems and gaps in defenses. By employing a fully integrated solution, MARCW has now eliminated the gaps between their security functions; by having that solution administered by Network Box, they have further ensured that there is no disconnect between the technology and those managing it. After experiencing a security breach first hand, Bruce understands that the key to being safe in the digital world is good security policies, multi-factor protection and constant vigilance. With a written policy handbook and a Network Box subscription, Bruce is confident that MARCW now has all three.

McCusker, Anselmi,  
Rosen, Carvelli  
& Walsh, P.C.

All trademarks are the property of their respective owners.

This case study was authorized by McCusker, Anselmi, Rosen, Carvelli & Walsh, P.C.

Network Box LLC  
Newport Financial Center  
111 Pavonia Avenue, 4th Floor  
Jersey City, NJ, USA 07310  
Web: [www.network-box.us](http://www.network-box.us)