Information Security Essentials for your PEO

Jason Heuer and David McCullough

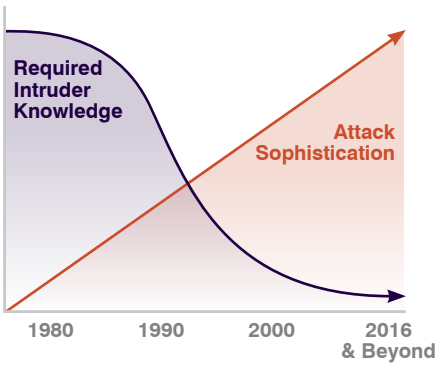
Nowadays, we don't need to tell you the importance of keeping your data secure. You read the headlines, just as we do. In the age of the information "cloud," it is easy to believe that your data is secure simply because it isn't housed in your office or on machines that you physically own. The reality is that the information is your responsibility to protect even if you have moved your infrastructure into a cloud-based solution.

Below are a few examples of the hardware and software solutions that we employ at LandrumHR to ensure that our data and networks are safe from intrusion. We also include a glimpse inside our thought process as we evaluated our options in hopes that it will help you as you work your way through the maze that is information security.

Intrusion Detection and Intrusion Prevention Systems

It's a given that firewalls and encryption are required to improve security, but you also need security systems that will monitor your network in real-time at multiple network layers to detect activity. When these tools observe any suspicious event, they produce alerts for the network administrators or take predefined actions to thwart the attack. In some cases, these systems can detect attacker activity even before the attack begins.

Intrusion detection is the process of monitoring the events occurring on the network and analyzing them for signs of possible incidents, violations, or imminent threats to your security policies. Intrusion prevention is the process of performing intrusion detection and then thwarting the detected incidents. These security solutions are available as intrusion detection systems (IDSs) and intrusion prevention systems (IPSs), which become part of your network infrastructure to detect and stop potential incidents. Because IDS and IPS devices sit in different spots on the network, they should be used concurrently. An IPS generally sits in-line with traffic at the perimeters of the network to help stop zero-day attacks,[1] such as worms, viruses, and malicious activity, in their tracks. An IDS product is installed inside the trusted network and will monitor internal activity, guarding against the ever-present insider threat, and lend greater visibility into security events, past and present.



Attack Sophistication versus Intruder Technical Knowledge. (Source: Citi Online Academy, Digital Security—Cyber Security and Fraud Prevention)

LandrumHR's Story

We learned that attackers have an in-depth knowledge and understanding of the technology, infrastructure, and systems they target. In addition, the knowledge an attacker needs about our network to launch a sophisticated attack is decreasing over time. This means that attacks are growing at a frantic rate and are more sophisticated, and it is important that we stay out in front of them.

Most attackers will take the path of least resistance. It's simply too much work to break through blocked or hardened systems, so they will embed and disguise attacks (even in encrypted traffic) through trusted communication paths allowed by the system or firewall. Email is a prime example of using trusted avenues to get inside the infrastructure, where an unsuspecting employee can execute an attack that essentially bypasses layers of security with elevated access.

We knew the traditional approach of merely having a firewall, anti-virus software, and encryption were not adequate to deal with the increased skill of the hackers and the threats that are constantly developing. Because LandrumHR operates in a hybrid environment of cloud services and local assets in the data center, we needed solutions that provide tighter controls over all traffic, as well as constant visibility into the state of the network across all services. LandrumHR prefers layered security because no single solution can realistically

1 Attacks that exploit a previously unknown security vulnerability, sometimes taking advantage of a security vulnerability on the same day it becomes generally known.

deal with threats that are coming from every direction and that could easily propagate at several network layers.

The concerns we were trying to address are:

- Increasingly sophisticated attacks;
- Compliance;
- Liability;
- Insider threats; and
- Lack of visibility across the entire infrastructure.

We knew that we had to make a major investment to address these new threats. This is where IPS/IDS systems come into play. The IPS allowed us to inspect trusted and untrusted traffic in-line and in real-time on multiple network layers and take immediate action to stop threats at the router or firewall. The IDS allowed us to get an overview of activity inside the network and identify malicious behavior before any damage was done.

Beyond IDS and IPS solutions, we recognized scenarios in which a trusted insider or an attacker that has gained trusted access could manipulate or leak data outside of the organization.

Like you, LandrumHR houses customer data, intellectual property, company data, etc. Housing that information requires a level of liability and responsibility for the security of that data. We had to ask ourselves about the potential of sensitive data leaking outside the company, assuming an insider has trusted access within the network. Employees are given access to sensitive data to do their jobs and would not typically be considered threats by IDS or IPS systems. How do we address something that is allowed while at the same time prevent abuse and exposure of sensitive information?

Specifically, the concerns we were trying to address were:

- Data theft;
- Compliance;
- Privacy laws;
- Controlling data sprawl; and
- The various ways data can leave the organization (USB, email, printing, websites, etc.)

Data loss prevention technology was the answer. DLP is a system that sits inside the network monitoring data at rest, in use, and in motion. Its purpose is to detect potential data breaches, or attempts to move data outside the organization's network and beyond its control. The system is based on our business rules and enforces those rules when data is accessed. The system can enforce rules as data is being read, copied to other media, printed, emailed, uploaded to websites, etc. We found the system not only prevented data theft, but also enforced business rules and compliance. We look for personally identifiable information (PII), banking data, medical, and other sensitive data and restrict its movement within our network. It has been an extremely effective tool in our data security toolbox.

As you might imagine, we went through an exhaustive evaluation process before deciding on our solutions. While the industry has some commonalities in data security needs, each company is unique. There are many options and the vendors are numerous, so take your time getting to know the players and how their solutions measure up to your needs.

After all of your efforts to identify and implement these software and hardware solutions, remember that these systems are not foolproof. However, they do significantly reduce the attack surface of the network. Don't overlook standard employee awareness training, continual penetration testing of your systems, and keeping up-to-date on the latest security threats so you can take precautions to ensure that your organization is as secure as possible. ●

Jason Heuer is IT director and David McCullough is chief administrative officer for LandrumHR, based in Pensacola, Florida.