The Secret to Embracing User Privacy While Stopping the Insider Threat

Dave DeWalt
Vice Chairman, ObserveIT
and Founder, NightDragon Security

observe it

The Secret to Embracing User Privacy While Stopping the Insider Threat

When you hear the word "cybersecurity," what's the first thing that comes to mind?

Do you picture a costly incident, perhaps involving a hoodie-wearing hacker? The day-to-day pains you face safeguarding your systems, files, and data with limited resources? Or maybe you're thinking about the cybersecurity tools you already use (and possibly hate)?

More importantly, which threats do you think about?

For years, the primary source of risk came from outside an organization's four walls. CISOs and their teams turned their focus to protecting valuable systems, files, and data from that external threat. But that's all shifting.

The insider has become the new outsider.

For proof, all someone has to do is turn to the news to see coverage of a high-profile insider threat incident, like that seen at Tesla, Amazon, Uber, or Google. And it all has to do with the agile workforce, rapid adoption of cloud technology, poor data security, and user privacy.

Applying Context

Why does this shift matter? Historically, spear phishing (among other outside-in approaches) was the best way for an attacker to gain access to valuable systems, files, and data.

In this outside-in approach, attackers would target an individual or company, using (in many cases) publicly available information about that target to appear familiar and trustworthy. Over time, their target would grow to trust the attacker, and take an action that gave the attacker an entry vector.

Sometimes this entry vector was malware in the form of a keylogger, capable of stealing credentials, so the attacker could access what they wanted and remain undetected. If that didn't work, attackers might attempt a breach of 2-Factor Authentication (2FA) vendors.

However, **a potential insider threat already has access to valuable systems, files, and data.** They don't need to appear trustworthy to obtain access. Trustworthiness is only needed if the individual is trying to cover their tracks (i.e., they're acting maliciously).

Addressing the Shift

If there is one thing that I've learned from my experience running some of the world's most innovative companies; including the founding of NightDragon Security and being an ObserveIT board member; it's that perspective and buy-in is everything.

We need to acknowledge that the average person only cares about what affects them directly. If they heard the word "cybersecurity," what would they think of first?

Password complexity? Installing and updating antivirus software? Avoiding malware and phishing attempts? Maybe being more cautious with his online activity? All of these stories have been huge in the cybersecurity space – continuously told by everyone.

But the ramifications of each have not always been apparent.

With a cultural shift in focus from the outside-in to the inside-out in cybersecurity, vendors and teams need to do a better job telling their story. Cybersecurity best-practices need to be relatable, digestible, and valuable to those who are at (or just are) the greatest risk: the potential insider threats.

As more and more high-profile data breaches, leaks, and misuse occurs; as well as the launch of new compliance regulations; the average person is becoming increasingly aware of (and concerned with) their own data privacy and security.

It's up to CISOs and their teams to meet their insiders where they're at, and embrace user privacy while stopping the threat.

Why Privacy Matters

The concept of user privacy with internet-based technologies is one that has been spoken about often but has been quickly brushed to the side over the years, as new companies and industries took advantage of lax regulations to create, innovate, and profit.

And there have been a lot of really substantial benefits of such an open use of data up until this point. But like the Wild West of the United States of old, the gun slinging, free flow, rough and tumble use of data has to end. The world is pushing things to become more "civilized."

It isn't enough to simply react to a privacy breach after-the-fact. Foresight and action are needed, and now is the time to start taking advantage. C-level executives are beginning to take note, and it's because of the widespread effect these incidents can have!

People, the real users and sole benefactors of data use, want to know more. Who wants their data? How will it be used and secured? What are the processes, technologies, and techniques being used to ensure its protection? And most importantly – what are the ramifications if something goes wrong, for all involved parties?

We've seen the proof of this "want" with the introduction and adoption of the General Data Protection Regulation (GDPR). The primary focus of this regulation was to deliver more privacy and control over how user data is collected, used, and shared.

It caused a lot of trouble for a lot of companies on a global scale. Some had to invest millions, if not billions, of dollars to become compliant. Others face potentially steep penalties following its enactment, including Google, Facebook, Instagram, and WhatsApp.

A few high-profile companies even went out of business. (Ever heard of Klout?)

Even beyond the scope of GDPR, we're hearing about instances where data leaks, misuse, and breaches are causing huge headaches for both companies and the users that they serve (and collect data from). Do the recent data and privacy incidents with Facebook, Google+ (yes, it still existed until recently), and Amazon ring any bells?

They all represent increasingly common scenarios where proprietary information, including personally identifying information for users, are exposed to unauthorized sources. Who knows what might happen with that data once it's been unleashed?

State sponsored threats are also on the rise, and we're beginning to see some potential interference and collusion with the way that the public uses digital technologies. It's only a matter of time before state sponsors take advantage of our lack of user and data privacy on the regular. (This reality is a huge part of why I'm investing so heavily in the cybersecurity space.)

Companies and individuals alike can be affected by data incidents.

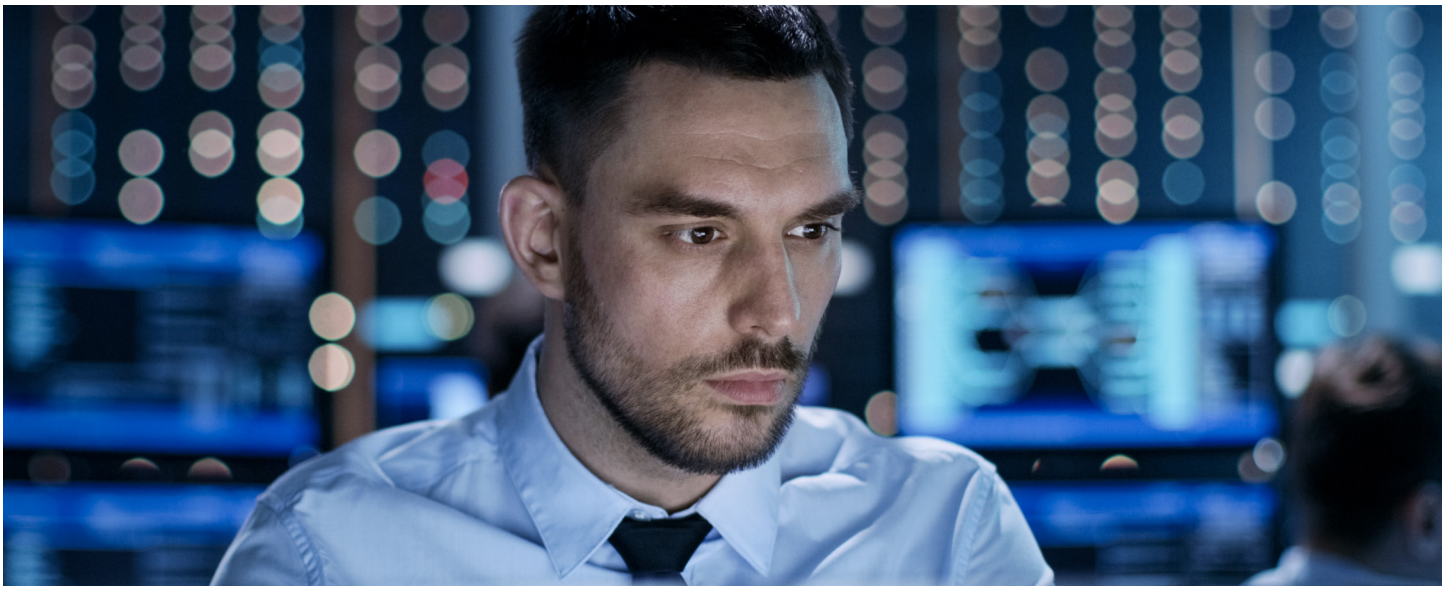
This is all important to call attention to because it shows how important it is to be mindful of user privacy and valuing data enough to protect it well. Failure to do so not only potentially impacts a company, but the people it employs and serves.

An example of this can be seen with the influx of healthcare-related, Personally Identifying Information (PII) data leaks. The moment data about someone is out there, there is little that can be done to safeguard it. Imagine if your name, home address, and other data was shared without authorization?

The question is: do you want to be responsible for a cybersecurity incident with such widespread ramifications?

Addressing the Insider Threat

An insider threat is someone inside of an organization, such as an employee, contractor, or vendor, who misuses authorized access to sensitive systems or data, either maliciously or accidentally, resulting in a negative outcome.



Due to their proximity to valuable data, controls, and distribution methods, the potential insider threat poses significant risk to the privacy of both an organization and its data sources.

This is particularly interesting because, from a historical standpoint, the insider threat has taken a backseat, up until this point, in the fight against data theft and misuse. Many organizations chose to primarily detect and prevent threats from external sources, and have invested heavily in the tools, processes, and people necessary to do it.

But when we consider the fact that the recent push for data and user privacy stems partially around the public need for transparency into who is doing what, and how with said data, the external (and internal) method of protection seems inefficient, if not useless.

The investment in external cybersecurity threats wasn't wrong, but it was incomplete.

So, it is curious that more organizations don't have visibility into what is being done with organizational data, and by whom.

When I invested in ObserveIT with NightDragon Security, I wasn't just buying into what they do as a company, but why they do it. There is a direct correlation between data privacy, organizational processes, and managing the potential insider threat. ObserveIT gets it – they're not only providing teams tools to help detect, investigate, and stop insider threats, but ensuring that an individual insider's privacy is not overridden or devalued. It's huge!

This is not to suggest that the data privacy problem can be solved by insider threat management alone – far from it. But if an organization implements guidelines and policies for data governance, knowing they're being followed is crucial.

To know that, visibility and context are key, and the right tool can help deliver that.

The Culture of Privacy

User and data privacy will continue to be a growing concern in the foreseeable future. There are very strong indicators of this with the aforementioned outcry over recent high-profile data leak, misuse, and breach incidents, as well as the forthcoming California Consumer Privacy Act, and talks of a U.S. specific federal privacy regulation akin to GDPR.

So, what can be done to start alleviating pressure to adopt more stringent privacy standards? And if part of the solution involves obtaining more visibility into what is being done with data, how, and by whom, how can the privacy of employees, contractors, and vendors be protected?

It all starts with building a culture of trust.

Creating a culture that lives and breathes it, and always strives to protect the privacy and security of data, files, and systems. Frankly, any good startup or organization seeking long-term relevance knows the value of building a strong culture. But it's up to all of us to integrate core values like privacy, trust, and security to make the places we work even more successful.

Education and Coaching

As can be imagined, to improve we have to be able to open up our minds to the notion that we just don't know everything. We only know what we know, until we know more.

We should always strive to learn more.

Something that has been missing from the world of cybersecurity up until this point has been the understanding that education is important. To adopt best practices, organizations need the ability to learn what is working, and subsequently, not working. **There needs to be a sense of understanding that the only way security can get stronger is if we all are capable of participating and have incentive to do so. This means that we need to lift each other up.**

I expect this mentality from the teams I worked with at my companies and investments, and it really is a necessary tool for success. (For those of you claiming that fear is a good incentive, you couldn't be more wrong.)

All of this can be applied to the concept of building a culture of trust, where improved data privacy and security are tantamount to an organization's success. To accomplish the education and coaching side of the process, you might:

1. Embed Privacy & Security into Existing Workflows

Change is scary to a lot of people, but if you can integrate these concepts into an existing workflow, adoption will be much smoother a process.

2. Use Real Stories

Stakes are one of the world's best teachers. Share real news stories with your organization to show cause and effect and relate it back to core values.

3. Embrace Trial & Error (to an extent)

Set up real-life workflow scenarios that call out failures (and successes!) of embracing privacy and cybersecurity in the workplace. Enable and encourage open discussion.

4. Coach Along the Way

Sometimes people need gentle reminders when they mess up or are about to mess up. By catching incidents as they are happening, if not before, you can subtly show team members the right way to think about (and act during) a situation.

Execute with Transparency

Rules without context are hard to digest for anyone, particularly if they stop or slow you down. (See: people who speed while driving, despite the posted speed limit, as an example.)

This is especially the case when it comes to security and cybersecurity measures. If a solution to a problem (such as insider threats) is cumbersome, or is not explained properly and with appropriate context, it just won't work. People require a certain level of transparency and stakes to buy into a concept. The current global user privacy and data security dialog is only amplifying this fact.

In a sense, it is all a matter of trust. Cybersecurity is also about trust, but it can't be one-way.

According to the 2018 Work and Wellbeing survey report put out by the American Psychological Association, 1 in 5 employees stated that "they don't trust their employer." That 20% is a sizeable chunk of people!

So how do we increase the potential for insider buy in to cybersecurity policy, while embracing user and data privacy, and minimizing the risk of insider threats? An open forum is a good place to start.

Consider talking with your teams about:

1. The importance of having cybersecurity policies (**value**)
2. The cost of incidents and compliance failure (**scope and weight**)
3. Explain who is affected when an incident occurs (**radius of effect**)
4. Causes of potential incidents (**how they are involved**)
5. What is being done to monitor compliance, and ramifications (**tools and response**)

There's a Star Trek quote that neatly describes the importance of buy in and building a culture of trust and cybersecurity acceptance: "The needs of the many outweigh the needs of the few."

If organizations embrace cybersecurity education, enforce user and data privacy, and keep an open dialogue with involved parties, there is a much better chance of minimizing overall incident risk.

Think of it as an investment in your people, your company, and your customers. A smart investment, if you ask me!

Use the Right Tools

Just knowing that you have a culture that embraces privacy and cybersecurity isn't enough. Verification that policies are being followed is necessary, from a risk management perspective. This is because despite our best efforts and intentions, there is always the potential for someone to cause a costly incident (malicious or accidental in nature.)

Many organizations already use a variety of tools that deliver visibility into potential external threats to their systems, files, and data. But not many include a look inward – to the employees, vendors, and contractors that also offer significant risk – the insider threat.

ObserveIT is an Insider Threat Management platform that empowers organizations to detect, investigate, and stop insider threats. It can help determine who, is doing what, when, and how, alerting you when a user is going beyond policy, or acting "riskily." It delivers context necessary for identifying insider threat-caused incidents or potential problems – a must for protecting user privacy and data.

As you'll recall, people always want to know more about how their data is being collected and used. The primary benefit of a tool like ObserveIT is for protecting organizational and customer data and assets, but it can also safeguard an individual employee, vendor, or contractor's data as well. ObserveIT can do this through a feature called: Data Anonymization.

The Data Anonymization feature randomizes and shrouds an individual's user and file activity with non-identifying classifications, so that cybersecurity teams cannot target individuals or misuse the information that they have access to. Instead, they must have a valid, verifiable, and trackable reason for requesting access to the insider's identifying data.

In other words, it is possible to embrace user privacy while stopping the potential insider threat!

In Closing

What's the big secret? It's simple: value.

The "Wild West" of the mid to late 1880's came to an abrupt end when the expansion of the established, industrializing, civilized cities reached the region by train. The free-for-all mentality that had previously flourished all but disappeared, due to the reality that people want to be able to live in physical safety and comfort.

The cybersecurity equivalent is a bit less direct, but the idea remains the same. People want to be able to benefit from digital services and technologies (comfort) but exist in relative safety. That's the value!

This is interesting, because people overwhelmingly have been using digital services and technologies despite a lack of relative safety up until this point. You can see this in the various cases of user and data privacy violations (i.e. leaks, misuse, breaches) among high-profile services like Facebook, Google, etc., and users continuing to use their services.

Usage rates may dip or drop, but so long as the bottom line isn't affected, the forcing factor for businesses to change hasn't been statistically relevant until recently. Likewise, the forcing factor for users hasn't been relevant, because in many cases people don't know that they have been affected by an incident.

Another example can be seen with the "Do Not Track" tool found within most browsers. A recent survey by Forrester Research (reported on by Gizmodo) discovered that while a quarter of users in the U.S. use "Do Not Track," most websites and services ignore it.

The main reason cited? No legal teeth or incentive for following through.

Despite this, the story surrounding the need for reinforced data and user privacy is bigger than ever. If you can deliver the value of safer, more protected data, you increase your organization's chances to succeed in the long run.

Will you lead the charge, or will your organization just be another left in the past? I've already made my choice. What's yours?

observe it