In today's world with ever-changing risk, it's not a matter of if you will be hacked, it's really a matter of when. And so in essential practice number two, the whole focus is on having situational awareness. We want to help our clients be more aware of the threats that are around them and how they evolve. We want to help them with the security analytics to understand all of the security data they're bringing in and provide a more rapid monitoring and response team to be able to address those threats when they do affect the organization.

When you think of the hackers, the "bad guys" out on the internet, they're brilliant. They spend all of their time, and some of them, it's really an eight-to-five job, they get paid to identify vulnerabilities and come up with exploits that can then be used to break into systems and steal data. For us as a company, as an organization, we're fighting an uphill battle to do that.

We need to do as much as we can to both be vigilant and informed about the changing threats, but also just really be on guard and able to respond and contain to them when they do occur because they will occur. It's much like in your local city or town, you have police, you have firefighters, you have first responders in case of any type of natural disaster. The same is true for a security team. They're going to be very aware of the threats that are present and evolving around that business and they want to make sure that they're ready and available to rapidly respond when that breach occurs. Every organization should have a security incident response plan, but that plan is not just a single checklist. It contains scenarios of the different types
of incidents that could occur, 
and because the threat is always evolving 
that plan needs to be continually 
maintained and updated. 
You learn from others, 
you exchange information. 
We have a program at IBM called 
the "IBM X-Force Exchange" 
where we can exchange and 
collaborate with our clients 
about what we're seeing in trends 
in information security 
and evolving threats. 
They can share the same back with us 
and we as a community 
become stronger for it. 
And the incident response plan 
is not just the responsibility 
of the security team. 
It takes the entire executive 
chain and company into account 
when they respond to an incident. 
So you have the actions 
the response team takes, 
you have the actions from 
the lines of business. 
You also often need to involve legal 
in case there's criminal or 
other legal considerations. 
And, often public relations. 
You need to make sure you're 
managing your organization's 
outward perception to both 
your business partners 
and your clients when an incident occurs 
so that they know that you 
are proactively responding, 
that you have the situation in-hand, 
and that they can continue to 
trust to do business with you.