Sarah Pavelek: Welcome to Plante Moran's Executive Series. Want growth? Embrace Risk. I am Sarah Pavelek, a principle in our cyber security team within in management consulting and I'm here to day with my colleague Colin Taggart who's a manager in the cyber security group as well.

Today we're going to talk about social media, the cyber security risks surrounding it and some suggestions on how you can lower your risk. So Colin, in our day-to-day work we see a lot of studies and research and study after study reveals when it comes to cyber security breaches employees are the most cited source of compromised information.

In your opinion, what do you think they are doing on social media that makes their organization so vulnerable?

Colin Taggart: That's a good question Sarah. The biggest concern we're seeing is that employees are now able to respond to customer comments without following any kind of marketing vetting process. So as customers have questions or concerns, any front line employee can now respond with possibly confidential information, inappropriate responses, just in general something that's not approved by the company.

Sarah Pavelek: Well, I think another thing too is that everybody talks about on personal pages, don't post that you're away on vacation, because then thieves know that your house might be unmonitored. Same thing goes for organization and company-wide stuff.

If you're posting that the entire company's away for the annual meeting, for example, it also opens you up to potential theft, physical attacks or even cyber security attacks when it comes to knowing that potentially the entire IT department is away and not monitoring as much as they often would.

Colin Taggart: Mm-hmm (affirmative). Also related to that, that monitoring process of even knowing what pages you've locked down, there are sights out there such as Google and Yahoo where you can claim those pages, change the hours, change the contact information, if you're not aware of anyone on your teams already claimed those competitor or someone who has malicious intent could change those and possibly damage your business reputation.

Also, looking at the IT side is even looking at setting up strong passwords, so for these accounts that are official for marketing purposes, have we set those up so passwords aren't shared with multiple employees and it's something a bit more complicated than just your company name 1 2 3.

Sarah Pavelek: Right, because if the password's not strong it makes it a lot more vulnerable to attack. And I know one of the things we saw recently was a very large fast food restaurant chain, their accounts got hacked and started promoting the

competitor's organization, so that's something I don't think that anybody wants to do.

Colin Taggart: And also With those accounts if they're not hacked, we've seen accidents happen with employees that use their same phone or laptop to post as their personal account as well as the companies brand image, so if they make the mistake of posting on their company account with something that should have been personal about their weekend plans or their political views, all of a sudden you have a company fiasco of what the official account is saying.

So with any of these procedures, whether it's marketing or all employees, a big piece is do we have policies and procedures regarding the best practices.

Sarah Pavelek: Yeah and I think that's a big thing is to make sure you do have a formal policy so that there is a formal social media policy that employees are aware of it and they know what things that they should and should not do. Colin, what are some of the things you've seen in a good social media policy?

Colin Taggart: One piece we usually look for is how we're monitoring everything out there. So again, whether it's the Facebook page the company has officially sponsored, how are we watching for customer complaints, customer questions there? What are we also doing to just monitor essentially the entire internet for any pokes about the company names?

There's a variety of social media monitoring tools out there that you can have in your policy that marketing will use XY and Z about what's being said about the company.

Sarah Pavelek: Yeah and I think that kind of goes to the whole culture of cyber security, so the policy is important but making sure that employees are trained on it and it's not just the what not to do or what to do but the risks and the reasons why you shouldn't do certain things. It just makes it a lot easier to understand the policies.

Because technology, you can tighten down technology but people are often the downfall. So you gotta make sure that people understand what the process should be and what they shouldn't do. Regular training, very, very important because it helps to drive home the message and I know one of the things that we do here in our office is we have bulletin boards and common areas, lunchrooms, cafeterias, busy hallways.

So, cyber security posters, something just saying here's a daily reminder of what the risks are, what you should and shouldn't do and I think that's a good suggestion for any company out there.

Colin Taggart: Thank you Sarah. That's a great point. That wraps up today's podcast. This is just one session in our five-part Executive Series. If you enjoyed today's discussion

we invite you to check out our other podcasts and webcasts on the following topics: Engaging the Millennial Generation, Business Disruption, Building and Preserving Wealth Amidst Uncertainty, Cutting Costs Without Sacrificing Quality.

You can access all of these at executives.plantemoran.com. Thank you again for listening.