Transcript

Wearable technology in the workplace: Are you wearing risk on your sleeve?

Gerry Kane, Cyber Security Segment Director, Zurich, and
Patrick Clarke, Assistant Vice President and Technical Director of Worker Health & Absence Management, Zurich

Voiceover:

Welcome to Zurich's RiskCast - **Wearable technology in the workplace: Are you wearing risk on your sleeve?**

Today, we have with us our Zurich wearable speakers Gerry Kane, Cyber Security Segment Director, and Patrick Clarke, Assistant Vice President and Technical Director of Worker Health & Absence Management.

We're talking about the rapid rise of wearable technology in North America, and how your company can prepare for the opportunities—and the obstacles—ahead.

Gerry, let's start the conversation with you….

Gerry:

Well, we're all pretty much aware that connected wearable devices like fitness trackers and smart watches are becoming increasingly popular every day with consumers. (Who do you know that doesn't have a fitness tracker!) Now it's industries' turn to embrace wearables.

The enterprise demand is so tremendous the demand for them is expected to triple in the next two years. (*Salesforce.com*)

But before we go too much further, Patrick, why don't you say more about what exactly wearable technology is.

Patrick:

Wearables are small, connected electronic devices that can be worn and operated hands-free. They provide access to real-time data.

They can stream live audio or video, track location and monitor worker vital signs, movement, heart rate, stress level and fatigue. These wearables can also monitor and operate equipment remotely, and much, much more.

The benefits are tremendous. They can generate real-time readings that help improve productivity, minimize project delays and speed up the decision-making process.

They're being used to help mitigate workers' compensation, disability and health exposure.

And the cost savings can be tremendous, which is why there is such an appetite for wearables right now.

For example, by some estimates, as early as next year smartglasses could start saving the field service industry $1 billion annually. (http://www.gartner.com/newsroom/id/2618415)

Gerry:

Yes Patrick, there's tremendous potential for smartglasses.

Imagine a doctor remotely consulting with another doctor during a procedure, or reviewing x-rays or medications, streaming real-time data hands free right from their smartglasses.

Or field industries with an aging work force and a high demand for skilled workers using smartglasses for remote training and collaboration.

Smart watches also have great potential. In manufacturing, managers can track inventory, check productivity issues, check quality control, troubleshoot problems, track shipments, get alerts when a machine malfunctions, check employees' schedules and location and assign work, all right from their wrists.

In healthcare, smartwatches can monitor nurse fatigue, lifting and movements, and other quality-of-care issues.

Patrick:

Instead of having to go back to the tool crib or job trailer, construction foremen or supervisors wearing smartglasses can pull up plans they're working on. It's a real time-saver and an efficiency gain from that perspective.

Gerry, construction is also very interested in wearable or sewn-in technology to track worker movements, fatigue, repetitive movements, forces and slips/trips/falls for worker safety. Construction is really intrigued by wearables, because the biggest loss exposures in the industry tend to be sprains and strains.

Gerry:

I'm seeing most industries in the exploratory or pilot stage, evaluating the use of these smart glasses or smart watches or smart clothes in multiple scenarios and job functions, and trying to understanding the efficiency gains.

Many of these devices provide great benefit in terms of productivity, efficiency, cost savings, safety or convenience.

But along with the potential benefits, companies also have to evaluate the potential risks. And we want to help our customers understand what these risks are and mitigate them.

Patrick:

There are huge barriers that really have to be well thought out before implementing wearables. Consideration for data collection and use, civil liberties, and the legitimate business need to use this technology is important. It really is a risk return on investment, or a risk on investment, kind of decision.

Gerry:

Consider that each one of these devices is a potential entry point for the bad guys, and that by some projections there will be anywhere from 25 billion to 50 billion connected devices in the next 4 years. That's just a staggering number.

Now the threat landscape expands astronomically.

Patrick:

Because everything is networked and anything networked can be hacked.

Gerry:

Yes! Cyber thieves don't have to hack your company's computers. They don't have to get into your network directly via a phishing exercise or other social engineering method if they can get into a vulnerable wearable device, because that device can probably get into a network that's connected to your network.

Wearables are subject to all the same threats that other devices have on the Internet of Things and in many cases are put into production in a very vulnerable condition. This is usually due to the importance of being first (or early) to market and shortcutting the risk management process to achieve that goal. Having vulnerabilities means that these devices are easily "hackable" until the vulnerability is removed or "patched", and patching is not an easy process for many of these devices.

We believe that for producers of these devices, you should be thinking about what are some of the things that could go wrong in the very earliest phases of product development, and start planning to address those vulnerabilities right away. Similarly, for organizations that are deploying these devices, good risk management suggests that you consider the risks of using these devices well in advance of purchasing them. In that way you can mitigate those risks and even force the manufacturers to address your risk concerns before you take the delivery.

Patrick:

You have to constantly be very diligent, the way this whole technology and innovation is working today moving very, very quickly.

When our customers come to us, we make sure that they understand the risks that exist and how to build in control points.

Whether it is cyber, product liability, bodily injury, civil rights or some other, there are always going to be risks. We haven't even touched on all of them.

Gerry:

Right, and again, you have to ask questions right at the beginning of the implementation process. What are you trying to protect and what could go wrong?

For instance: What happens if the information in your wearable device gets hacked? And what happens if information is disseminated inappropriately?Or, what happens if a company implements technology and something goes wrong? Or it's reporting information incorrectly? Who's responsible for that? Is it the manufacturer? Is it the employer? What are the confidentiality and civil liberty issues?

What if a worker is using smart glasses and is distracted by it, and gets hurt on the job or accidentally injures someone else?

Plus, there are business continuity risks. If you're using wearable devices in the course of some vital part of your operation, and that technology is no longer available or was defective, how does that impact your business?

Patrick:

You're never going to mitigate it all, especially with the risk inherent in emerging technology like wearable devices. There are never going to be perfect solutions.

It's important that companies incorporate policies and procedures that vet any new wearable technology just like any other risk management initiative.

Gerry:

That's right, Patrick, and there are cyber risk frameworks available to guide this process. At Zurich, we think the NIST Cybersecurity Framework is one that is very effective and is based on five high level activities: Identify, protect, detect, respond and recover.

Start by IDENTIFYing exactly what it is you are trying to secure, whether it is data, processes, communications, or even people and physical objects. Perform lots of risk assessment to identify all of the threats. Once you've done that, establish controls to PROTECT what you have IDENTIFIED. But as you said just a minute ago, there are no perfect solutions—no 100% protections. So you must have monitoring capabilities to DETECT when something has, or is about to, go wrong so that you can RESPOND to that condition and RECOVER to normal operations.

If you've got a solid framework in place, you can manage the changing technology by sticking to your processes.

Voiceover:

Learn more about wearable technology, and what your business can do to protect the things you love. Visit us at **zurichna.com/wearables**. Thank you for joining us.

Sources include Salesforce and Gartner research, the Risk Management Society, and the World Economic Forum's Global Risk Report 2016.