Broad Matters Season 6 Episode 1

"Cybersecurity in the Supply Chain" with Steven Melnyk

Ken Szymusiak:

Welcome to Broad Matters.

Amy Wisner:

A podcast bringing you thought leadership, innovative perspectives, and real world impact from Michigan State University's Eli Broad College of Business.

Ken Szymusiak:

I'm Ken Szymusiak, managing director for the Burgess Institute for Entrepreneurship and Innovation.

Amy Wisner:

And I'm Amy Wisner, business communication professor in the department of marketing.

Welcome back listeners, Ken and I are excited to be kicking off another season of Broad Matters. Joining us today on the first episode of Season Six is Steven. A. Melnyk, professor of operations and supply chain management.

Steven Melnyk:

As long as I've been here and I've been here a good long time, what makes Broad different is we've always developed a close working relationship with industry. And by being close with industry, you identify potential problems and we can act, develop, educate our students about what to do with those issues. Broad matters when you want to have an impact. Broad Matters when you want to understand what is actually taking place rather than what the book tells you. Broad Matters when you understand that the importance is not generating the number, but generating the desired outcome that helps the organization achieve its goals. We challenge our students to take that number and say, how would you use it? How would you change things? We expose our students to what is actually taking place, not what the literature tells us is taking place. That's what makes us different.

Amy Wisner:

He's been at MSU for over 40 years, lending his experience in operations management to identify and address issues that business managers face every day.

Ken Szymusiak:

Welcome to the podcast, Steven.

Steven Melnyk:

Thank you for having me. I'm thrilled to be here to talk about my work and to highlight some of the issues we're now looking into and why they're important to supply chain now.

Ken Szymusiak:

Thanks for joining us. Could you start by just telling us a little bit about yourself and your work here at the Broad College of Business?

Steven Melnyk:

Senior faculty like myself, have traditionally been charged with the task of being pathfinders. Our goal is to identify, evaluate, describe new and emerging areas for research that others can fall into. And that's something which has driven my research over the 40 years I've had here. So what I've done in that time period is I focused on answering a simple question: what keeps the business manager up at night? And it's that question which has driven my research, first of all into scheduling and then into shop floor control and then computer and game manufacturing. And then I was one of the first researchers into sustainability. And then now I'm one of the first researchers talking about cybersecurity across the supply chain. I'm leading a coalition of researchers which are now looking at an interesting topic, which is supplier separation. Looking at why in today's environment, suppliers fire customers and why customers have to care about that.

Ken Szymusiak:

That's awesome. You've gotten to experience essentially such a broad variety of research topics through your time here. And so this is going to be a really interesting conversation. I think we should start with one of your last prompts, which was cybersecurity and supply chain. I think a lot of people know what the term cybersecurity means now, right? Change your passwords. Someone steals my identity, from a personal perspective, but how does it apply into the business world? Especially when you think about supply chain security.

Steven Melnyk:

Now you asked a very good question, and let me restate the question. Why should we care about cybersecurity? The rate of cyber crime is increasing. Give you some statistics. 68% of all firms have experienced some form of cyber attack. By the way, what's really interesting in responding to the survey, 36% of the executive team felt that investing in cyber protection was irrelevant. Didn't get that one. Cyber breaches have increased by 11% since 2018, and 67% since 2014. One cyber attack occurs every 11 seconds, twice the rate of 2019, which was once every 19 seconds and four times the rate in 2016, which was once every 40 seconds. In today's world, which is now dependent upon responsiveness, sustainability, resilience, efficiency, innovation, those connections are really critical. They're both our strength and our weakness. There are six reasons we should care about cybersecurity.

The first is we're all vulnerable to it. And what do we mean by that? Well, number one, data is becoming increasingly more important. And that data is not simply things like passwords, it is specifications for designs. It is how you work with your customers. It is bills and material, its cost structures, it's the operating instructions that you send to your equipment to build parts. It's kind of interesting to note that in talking with managers, one of the things we found as a result of the pandemic is that the old model of working at the office is becoming less and less attractive to many employees, which means they want to work at home. But to do so, they potentially expose sensitive data to observation from others. And that can be important. So the first thing is we're all vulnerable.

Number two, industry is now interconnected. I remember some years ago I was at a presentation done by one company and what they described is the fact that they had gone from an eight to five environment to a 24 hour environment. And what they had done is described a problem. The problem's identified in California. And when the people got ready to go home, the problem didn't stop. It was passed to their facility in Australia. It was then worked on, digitally worked on, then it was passed to India where it was again worked on. Then it was passed digitally to Europe, where it was worked on again, then it was passed digitally on to the United States where it was worked on again. And that was important to the company because the problem was being addressed in real time continuously but what

made it possible was the digital interconnectivity. And also it's important because nowadays what we're now doing is we're sharing data with our suppliers and our customers, which means I pass a design to my supplier and in that design I have maybe intellectual property. And that becomes the basis on which they work.

So suddenly you start to see that in today's environment, industry 4.0 is based on the promise of responsiveness and customization made possible by digital. And also we're starting to see the fact that IOT has changed the game. IOT is the internet of things. What you're seeing is we are in living in the digital real-time world.

The third reason is we have to recognize as significant economic impact. It's estimated that at the end of last year hacks across the world, direct costs were in excess of 6 trillion dollars, US. In addition to that, a recent statistic came out of IBM is that a successful cyber attack can cost a firm up to $13 million to detect and mitigate. And finally it takes 276 days on average from the time that the attack takes place until it's successfully contained in the United States. So those things are making things nasty.

Phishing attacks, et cetera, identity thefts are becoming more important and it's also a threat to national security. It can be used to disrupt national and energy infrastructures. In May of 2017, the Russians launched a cyber attack against the Ukraine. It was called the NotPetya attack. And what it is, is NotPetya, it's based on the virus, except what they had done with the virus, they turned off the key.

Most viruses have a key that you can turn it off or on. What they did is they targeted energy, hospitals, government, finance and education. They're going after infrastructure. Remember I talked about how companies are interconnected?

Ken Szymusiak:

Mhm. Absolutely.

Steven Melnyk:

This means an attack that takes place in one area can jump to another area. And at this time, I was teaching a program in Rotterdam and I had someone from Maersk. And what had happened is one of their operations had gotten infected with a NotPetya antivirus. Why? Because they had a terminal located at the hospital in the Odesa, Ukraine. That virus jumped from the hospital to Maersk and it propagated all through Maersk.

She was describing what was happening. IT people running up and down the hallways, telling people to turn off their computers, not even to turn them on. Because if as soon as you turn them on, you brick the computer. Guess how much that attack generated in terms of collateral damage?

Ken Szymusiak:

Billions.

Steven Melnyk:

10 billion.

Ken Szymusiak:

Yeah.

Amy Wisner:

Wow.

Steven Melnyk:

And the final issue is the government, the federal government is focusing on it. They've introducing CMMC, which is cybersecurity maturity model certification. And in March of 2020, a joint partisan committee issued the cyberspace solarium report on cyber security. It's available online. I would strongly recommend that your listeners get into it. And what was interesting is it strongly emphasized the fact that warfare as we move into the 20th first century is going to move from destruction of buildings and people to destruction of digital infrastructure. And one of the things that's interesting from a supply chain perspective is out of the 80 plus recommendations, over half of them were on supply chain. So how's that, why you should think about it?

Amy Wisner:

That's really interesting, Steven. Can you tell us which areas of the supply chain do you see as being the most vulnerable to cyber risk?

Steven Melnyk:

The answer is the entire supply chain. Because the fact that companies are attacking firms through the weakest link in which is often a small supplier, that supplier is at risk and the rest of the supply chain is at risk. When people attack the smallest supplier, they create a condition which is problematic. And what's that? The small supplier, because they often lack the expertise or the money are unable to provide adequate levels of protection. They get attacked. Then they create what's known as the supply chain externality, which is the hacker attacks them, they create a problem for someone else, but they don't incur the costs. For the risk to be eliminated, we have to mandate that that supplier invests to eliminate the risk. And in that very condition we create one of the weaknesses in the supply chain. We run the risk of losing the supplier.

And so the first thing we're trying to see is: this is a supply chain issue. Once we see it that way, we start to understand that it's forcing us to deal with an issue that we have avoided for the last 20 years. That is, managing beyond the first tier. In most supply chains, I manage one up, one down, which means I work with my customer, I work with my supplier. When I work with my supplier, what I do is I say, you are responsible for managing your supply chain.

Number one, we have known since 2011, that does not work but why have we done it? Because it's quick, it's cheap, and everyone else is doing it. Guess what we're finding out? We got to do it. Increasingly, supply chain visibility is becoming a critical issue. So that's why I said it affects everything. And in the process we're starting to understand that the issues we do for cybersecurity are not unique to cybersecurity. They become important for visibility.

Little point, I'm going to differentiate between two types of visibility, active and passive visibility. Passive visibility is you're in a train that's running far ahead, but you can't do anything about it. When I use technology, I'm doing passive visibility. Active visibility, I'm in that same train, but I can affect its actions. The first part is technology, it's IOT, it's big data. The second part is relationships. Are you a good customer? Does your supplier trust you? Is your supplier willing to work with your second tier supplier? That's the real battle we're starting to find. The thing that we worry about with cyber is the same thing we worry about with visibility. And we need visibility because number one, the customer wants it. Firms want visibility because it's a way of managing risk. So you can anticipate problems.

Ken Szymusiak:

My grandfather's business was a supplier tier two, right? And the layers of complexity and the amount of pressure on the major suppliers will put on their suppliers, on the tier two, tier three is… it's brutal. And every piece along that supply chain, the margins are even thinner. And so when you think about how those companies have come to rely on almost single-source customers to some extent, how do you kind of escape that trap now? It's almost like a total culture change I feel like needs to be bought into.

Steven Melnyk:

That's a good question and the reason it's a good question is because it's starting to recognize the shifting base of power. Before the pandemic where supply was assured, the power was with the customer. So we had things like the customer driven supply chain. I wrote about that early on. Now the power is going to the supplier because supply is no longer assured. And what's interesting is we're starting to see good suppliers firing bad customers. So we start to see that you had to excel at relationship management, you had to excel at supplier communication, you had to excel at commitment to the supplier. So the game has changed. So that's why we're looking at it and that's why cyber has changed and that's why you're starting to see that the issues that we're dealing with cyber are not unique to cyber. They're unique to everything else.

Ken Szymusiak:

Steven, this has all been really interesting content that we've talked through today. When you think about where our supply chain leaders are headed in the future, I think traditionally people think of supply chain as a tactic, but what you've been talking a lot about today is strategy. Which one is it?

Steven Melnyk:

10, 15 years ago, I would say we were tactical. Supply chain was about getting things delivered faster, better, cheaper. Increasingly, companies I'm talking with at all levels are focusing on the fact that supply chain is strategic. It affects how consumers view the company. When you have a shortage and you go into a place to buy something and it's not there. When you have a problem with a product and the company basically doesn't give you a good answer. Those are things that affect how you view it. That's by definition strategic. Recently I was at the NextGen Supply Chain Management Conference in Chicago, and this brought together some of the leading organizations in the world. And one thing that emerged over and over again was that the supply chain and the world has changed. When we look at companies like Procter and Gamble, we see companies which do not see supply chain as tactical, as strategic.

They knew about Ian coming into Florida. They used predictive analytics to identify number one, who were their three customers. Basically it was Kroger, Publix, and Costco. They then went in and found out what were the products they were going to use and they made forecasts. They were within one day of that forecast, which meant when everyone else was trying to get product out, they had the product in the hands of their customers, which meant that that was a competitive advantage. And so we're starting to see that it's becoming strategic. It affects how the company competes. It affects what the company can and cannot do. It affects the value proposition. That is strategic.

Amy Wisner:

All right. This has been a lot of information. So if you could say one thing that supply chain managers could do right now to improve their operations, what would you encourage them to do?

Steven Melnyk:

Oh, that's a question I can't answer because we have a systems problem. And what we've learned from history is that silver bullets don't work. What I'm going to simply say is, number one, today's environment is a great time for companies to reassess their supply chains because everyone knows that the supply chain as it's currently configured, does not work. One of the things we've learned from history is that unless there's a compelling reason for change, people don't change. Number two, this is time for us to reevaluate not simply how we buy, but how we manage relationships. And number three, this is a time for us to, in essence, identify the weaknesses that we see in the supply chain and ask the question, how do we rebuild the supply chain to ensure that those outcomes which we think are critical, are made inevitable? And those are fundamental challenges.

They're not unique to industry. I'm seeing them in the government, I'm seeing them in defense, I'm seeing them in the private sector. So this is a good time. And this is a time where you sit back and you ask the question: what is it that you want your supply chain to do? And we're finding out that cost, which used to be important, is no longer enough. It's now issues like sustainability, it's issues like responsiveness, issues like resilience. It's issues like innovation. It's issues like security. And the funny thing is no supply chain can ever do all of those well. So this is the time for us to ask the question, what do we want our supply chain to do? What I've been doing is focusing on just one answer. Security. Is it the only answer? No. The answer I'm offering you may not work, but the question still stands. What do you want your supply chain to do?

Ken Szymusiak:

Well, thank you so much, Steven. This has been really interesting topic and thanks for talking with us today. How can we keep up with your work going forward?

Steven Melnyk:

Basically, send me an email. I'm working currently with various ways. I publish frequently in Supply Chain Management Review. My readership is much more practitioner oriented and I can get published much more quickly. So my research is timely. Research right now in academic journals is two to three years, and in today's environment, that's death. "The problem is over, but we've got a solution."

(Laughter)

Anyway. The other thing too is keep in contact. Send me an email. We have a mailing list because I'm doing research on not only the issue of cybersecurity across the supply chain, but on a related topic, which is supplier separation. Understanding why suppliers fire customers with the idea of being able to identify suppliers at risk. And the source of my questions has always been industry. Like some of my colleagues in other schools who look at research, I look at industry. Let me give you the analogy I use: They're looking at cadavers, I'm looking at real bodies.

(Laughter)

Ken Szymusiak:

Awesome.

Amy Wisner:

Follow us on Twitter, LinkedIn, Instagram and Facebook at MSU Broad College. Or visit us on the web at broad.msu.edu/news.

Ken Szymusiak:

And remember, like, rate and subscribe to Broad Matters on Apple Podcasts, Google Podcasts, and Spotify.

That does it for this episode. I'm Ken Szymusiak.

Amy Wisner:

And I'm Amy Wisner. Join us next time to hear faculty and staff weighing in on relevant issues and discussing how their work makes an impact. Illuminating how and why Broad matters.