InTransition ep 141 with Laura Bell

Speaker 1: Welcome to InTransition, a program dedicated to the practice of content communication in the public sector. Here's your host, David Pembroke.

David Pembroke: Hello ladies and gentleman, and welcome to InTransition, the podcast that examines the practice of content communication in government and the public sector. My name's David Pembroke, and thank you for joining us once again. Today we look into the thorny and very topical issue of cybersecurity, and particularly cybersecurity in government, given that most of our audience is working in government, and thinking about the content that they're creating, and also that the interactions and the technology, and the information technology that's now being used. And indeed, how they can think about this issue of cybersecurity.

Because today we speak to one of the world's leading authorities in the cybersecurity space. Her name is Laura Bell, and she is the CEO of SafeStack, which is a New Zealand based information security agency that focuses on protecting citizens and businesses online. It's a boutique security company, but it's really about planning and implementing those measurable security programs into your business or your government agency, so that you can keep yourself safe.

She also looks at this challenge of training people in security and cybersecurity, so as that people can know just exactly how it is that they can keep their organisations and their information and their content safe. Laura's also a board member for Hackers Helping Hackers, which is an Australian organisation based in Melbourne, which is promoting ethical hacking.

She, before founding SafeStack in 2014, Laura worked with a number of security firms, looking at things such as security assessments and the development of training, and also that critical role of information protection. She joins me now from Auckland, New Zealand. Laura, thanks very much for joining us InTransition.

Laura Bell: It's lovely to be here. Thanks for having me.

David Pembroke: It's a big issue, isn't it? Cyber. It's this notion of cybersecurity, and again, for a lot of people working in government, it's a huge challenge. Obviously there is at one end of the scale where you have organisations, particularly in a place like Australia, like the Australian Signals Directorate, that are really fighting the battle on the frontline on a daily basis, all the way through to people learning about their information management, learning about their processes so as that they're not leaving any weaknesses in their systems such that they can be penetrated by people who might be looking for information that they're not entitled to.

Laura Bell: It's a huge area, and it's an area that we don't really understand as humans very well. When you've got, say a giant eight-foot bear that walks in your door and looks at you with a hungry look on their face and just looks forward, you know exactly what you're dealing with. You've got an instinct built into you to protect yourself.

When we talk about cyber risk or cyber threat, we're talking about an ephemeral enemy, if you will, if you want to carry on with the military style acronyms and analogies we tend to use, that we can't taste, or see, or feel. We have no idea how big or small it is, where it’s coming from. So, it's a very abstract concept when we try and figure out how to protect ourselves, and that's led to some real challenges in knowing where to spend our time and money.

Because how do you do it when you don't have this kind of measurable feeling for what is out there and why you need to care?

David Pembroke: So how do you then turn it into something that's real? How do you take that ephemeral concept of, "I'm not quite sure what it is, but I have to think about it" to something, "Well, here are some concrete steps that I can actually take in order to deal with this threat?"

Laura Bell: Well, for us, we consider language to be really, really important in this space. Now, we all talk about cyber in this way at the moment that it's quite big and it's quite generic, really, in terms of what we're talking about. It could mean everything from a bored teenager who just doesn't have a lot to do on a Saturday night, through to a giant government agency who's decided they're going to pick a fight.

So, at SafeStack we focus on bringing this much more closer to home and removing the big fluffy language where we can. For example, if you talk about yourself as a human, rather than just at your work at the moment, you went into your living room, we like to work through exercises or organisations with individuals where we plan the robbery of their place.

It's a very dark subject, I'll admit. We're not the most fun at parties, but we will talk to them and go, "Okay, so what's the most valuable thing in your world right now?" That could be data; it could be a person, it could be a place. How would you steal it? We don't mean the tech; I don't want to hear words about port scanners and crazy hacking tools. It's irrelevant. It's how you would do this? Because the real thing about understanding and surviving security is demystifying it and realising that crime and theft is the same as it's always been with humans.

It's the path of least resistance, the easiest way we can do it, and so by looking at how we would attack, we can learn how we would defend.

David Pembroke: Oh, wow. Okay, so that's really the basis of it is the strategy about understanding weaknesses and how you can exploit those weaknesses.

Laura Bell: Absolutely. I've had CEOs of banks plan bank robberies. I've worked with people who ... We talk about some of the things we're not allowed to talk about. Why would you do extortion? Why are key people risk a real problem? Not to scare people, a fear for us is actually a pretty perverse motivator. You only get a result for a very short period of time, but it's once you start talking about that and normalising that it's okay to talk about, that we're vulnerable, and that that's scary, then we can then move on from fear into actually doing stuff, and it's the doing stuff part that we really need to get on with.

David Pembroke: Okay, so in that doing stuff, 'cause I think that's a great way to frame the challenge, so as that I now know, say I'm working in government, I'm a government information worker, I understand that there are vulnerabilities, but what are then the steps we've got to take, those concrete steps, in order to ensure that we're not contributing to a preexisting problem or that we are perhaps even establishing best practice in the teams that we work with?

Laura Bell: Yep. So, there's a couple of things in the space that we all need to take a breath and acknowledge. Firstly that best practice is fiction. Best practice is a very fluffy term that consultants like me have bandied around for years, and it's normally to disguise the fact that we weren't quite sure. And that's okay. Admitting we don't know is actually part of a security problem right now, is we're very scared of saying we don't know.

Regarding tangible steps and things we should do, it's very challenging for us to admit as a community, but it's the basics that are getting us every time. The ASD, the equivalence in the UK and New Zealand, have all put out lists of the types of vulnerabilities that are most likely to get you compromised. I think the top four controls for the Australian system were basic things.

They were updating and patching, managing accounts, that kind of thing. It's those basics, those simple things that we aren't spending the time on. We are spending the time buying devices and very sophisticated technological solutions, but actually if you can give $10 to somebody to trade for a password, or if you've got staff members who don't know how to handle information just in a basic, manual way, then we're wasting our time because we'll always be compromised by the simplest weakness, not the most complicated.

David Pembroke: Do you see that, well, in your experience, do you think that people see cybersecurity as their responsibility or is it something that the ICT department is responsible for. "Therefore, it's not my issue, and it won't be my fault if something goes wrong."

Laura Bell: It's funny you should say that. I think there's a bit of both. For example, if you take fishing, so sending emails to try and elicit materials such as usernames, passwords, documentation, and there's been rhetoric, a conversation in the industry for a long time, that this was because we weren't training our people. They didn't know what they should be doing, and some people, that's true, but we've actually encountered that 15% of the people that we've surveyed, and we've surveyed a number of organisations now in seven countries, we found that some of them were clicking the links on phishing emails, not because they didn't know any better, but because they were curious to see what would happen, because it wasn't their problem to clean it up.

They weren't incentivized, or they didn't have any ownership to say that this was a problem that they needed to care about, that they wanted to protect their organisation. I think that's quite a challenging message for us to get across now, is why we all need to care.

David Pembroke: In terms of that, though, and at what point should you be designing those interventions around awareness and understanding? Is it at the point of orientation where someone joins your team, and then sustain that over time, not just the, "Once at the beginning, and there it is, and we won't talk about it again?" What is the best way to be able to inform people, educate people, and then keep them engaged?

Because as the digital transformation continues to change, we have further improvements in technology, driven by the various components of artificial intelligence. Obviously, it's going to become, the threat will evolve and emerge, so how do we make sure that people are aware and able in this fast moving environment?

Laura Bell: That's a great question. I don't think there's one best way. The cop-out answer is there is no one good way, but there are some themes to what we should be seeing. Security, like any other defence, is a collaborative sport. It's a team effort. So, we need to plan our approaches to be collaborative instead of the isolating ways we do it now, such as eLearning on its own. Just making somebody click left 27 times until they complete a test isn't teaching. The entire education community rolls their eyes at us when they see how we teach our people.

We need to find ways to engage people that suit their role. If you're talking with people who are in call centres and they are incentivized in their role to keep people happy, that's their measurement of success for their day is customer satisfaction, then we need to plan our training and advisory for those groups so that they can still do their metrics, so they can still meet their targets, so their customers are still happy.

At the moment, we give very generic training to all our staff, regardless of the role. We don't really measure it's changed any behaviours other than the odd phishing campaign, and we certainly don't do any kind of action mapping where we look at the person's world and go, "All right, what do they care about and how do we fit in with that?" We dictate rather than collaborate, and I think that's the key. It's ongoing engagement by collaboration that suits the roles.

David Pembroke: But how then do you move it from that inappropriate teaching model, perhaps, to be able to say, as you say, an eLearning module, tick it, "Okay, you've now passed the test," to actually understanding that it is this ongoing, iterative process that needs to be embedded in the day-to-day activity of an organisation over a longer period? How do you achieve that change if we've got a current state that we know is inadequate and a future state that we know what is perhaps the best way to go about it, how do we encourage organisations to go from one to the other?

Laura Bell: I think for me, there's a couple of things we're missing at the moment that will help get us towards that point. I'm not sure we know what we need because we don't know what we're doing particularly right now. We don't have a lot of visibility, and that's the first thing. In your organisation, we have on average, security incidents, or security things we do are largely siloed into the team who deal with them.

Or, if we have a penetration test, or we have an event, it's kind of need to know basis. On the whole, the organisation tends to be very unaware that anything's going on around them most of the time. We never celebrate success, either. The security industry never celebrates us. We're kind of the anti-Christmas. It's because we're always failing in some way. There's always somebody breaching someone somewhere, but by never celebrating, by never calling out behaviours that are actually good, we only ever have a voice where we're negative, and that's not an engaging message.

So, having visibility, and not just in the negative sense, but also celebrating some of the positive, which is out there, and then we also want to have some measurability. If your department, or if your organisation is seeing a drop in the number of phishing attacks that worked, or the number of ransomware cases, or if you're seeing an increase in the number of people raising tickets or questions about security things, that's interesting.

If you're seeing more engagement in your documentation, are more people viewing your policies or engaging with your security processes? Then, let's see it. Let's measure that. Because if we're seeing and measuring, just like any other innovative business right now, the key to their success is measuring what they're doing, and iterating if it's not working. I think that will take us from what we're doing now, which is kind of we deliver our training in hope, to something we can go, "Is this working? Are we getting the return on it? What can we do differently to engage these groups that we can see measurably are not engaged right now?"

David Pembroke: Okay, that's fantastic advice. Tell me then, really, at a broader contextual, if we go up from the 50,000-foot view and looking down on this particular challenge, how big a challenge is it now and how bad is it going to get in terms of security around our information?

Laura Bell: I don't know how bad it's going to get, but it's going to get a lot worse before it gets better. For me, my personal research and the areas that really fascinate me are the new emerging technologies coming through, the machine learning back systems, the artificial intelligence based things. Not because of the hype and the buzzwords, but because at the moment we struggle to perceive all of the risks in an environment, and these environments are largely fixed systems.

If you put input in, you've got a system that does X, Y, and Z. You know what's going to come out the other end. We're literally building technologies now where we put input in, we have no idea what happens somewhere in the middle, and somewhere something comes out the other end, and we hope it's good. So, when you're trying to look at risk in that system, because you've got no clearer idea of consistency of what pathway that data is going take through your organisation, or what's going to come out, then we've got unknowns.

I think in terms of information, we are gathering more than we ever have, and it has more value, which is not news. But what's new is the fact that we are anonymizing and aggregating so much of it. We've never done that before. Like any other risk behaviours, the more you bring things together, the more chances are that risks will cluster together in it. So, we will start to see increased risk from de-identification of data, so crossing over from security into privacy.

We'll see increased repercussions if there is a breach, because suddenly the datasets are not affecting 3000 people, but millions of people. I think the first people to really automate and use this data for their own benefit will not be the well-intentioned. It will be the people who can exploit it for their own personal gain, whatever that is.

David Pembroke: Are there, this sort of almost caricature of these evil actors who are on a daily basis, seeking to create problems, whether it's in attacking an energy system or a major bank, or a telecommunications, or a defence network. Is that real, or is that just cartoonish, really, in the way it's characterised?

Laura Bell: There's an element of truth in it. There are definitely organised nation-state and organised crime gangs who are interested and very motivated to be in and around these systems. In the government space, more around the nation-state than the organised crime, but still. There's definitely truth there. However, not all organisations face the same kind of risks, so a hydroelectric dam is not going to have the same people interested in it as say a retail chain.

A retail chain, for example, if you attack it, you don't want to break it. A retail chain is very profitable to a criminal if you keep it alive and healthy. In fact, it's symbiotic. So, organised crime definitely wants a piece of that, but they want to sit their quietly in the background, doing their thing and making their money.

Nation-state actors, not really interested in retail chains. It's just not their thing. It's about finding out why you're valuable, and to who, and it's not the same people for each of us. That's actually kind of fun, if you can sit around and start thinking about who are those groups and what do they look like? You can come up with your own little personal most wanted list, if you will.

David Pembroke: Just explain to me, say this notion of a retail chain, and organised crime, and cybersecurity, and how might an organised crime gang penetrate a retail chain system and how might they be able to do that in such a way that they are undetected, but at the same time, they're accomplishing what they are, which is to obviously remove resources out of the retail chain into their own pocket, so to speak?

Laura Bell: Okay, so now for full disclosures, not talking about any particular retail chain, just in case anybody's sat there going, "Oh, my goodness." If it does sound like your world, I'm very, very sorry. Have some hugs for Christmas or something.

So, how would it work? Well, retail chains have things of value, so you've got different ways you can get value out of it as organised crime. You could get value out by stealing goods, so fake orders, get the goods, sell them, make a profit. You've got money laundering, so buy goods legitimately, but using perhaps stolen cards or some other form of currency.

Then either return them or on-sell them to get the money back, which is a really great way of keeping money squeaky clean. You've also got theft of credit card details to begin with, and with us entering a more aggressive online economy now, credit card details are a very lucrative target.

In terms of how and when they compromise, it depends on the business. All of our organisations now, retail and others, are built of hundreds of different technical components, each of which needs to be updated and patched and managed. So, finding something that has a vulnerability in it, such as outdated data software, or a poor password, is just a matter of time.

What we've actually seen in the past is that they will use either a legitimate account or some out of date software. They will gain a foothold inside the systems, and sometimes they'll even make a little cosy nest. They'll clear out other people who got their first, if there are other malicious people in there, patching up the things that could make them more vulnerable, and set themselves up and listen. Essentially, they're there to listen, see data, and then take it out to their own ends.

For retail, the aim is to stay in the system as long as humanly possible so that you can get the most benefit. Now, if the statistics are to be believed, from Gartner and the like, they estimate it's currently over 200 days between initial compromise and an organisation realising they've been compromised. That's quite a long time to get data out of a system.

David Pembroke: Oh, my God. That's frightening, isn't it?

Laura Bell: Absolutely.

David Pembroke: That's terrifying. 200 days before you actually know that someone's been in your house, so to speak, gathering information.

Laura Bell: It's phenomenal. For most people, they don't know how to come back from it. Most people don't even have logs that go back that far.

David Pembroke: It's sort of demoralising a little bit, isn't it? You think that people that have the sophistication, the skills, the time, the motivation, can apply that in obvious ways that are not positive, but then you as someone who's trying to resist that threat and attack, you maybe don't have quite the scale or the skill or the ability to repel.

Laura Bell: Absolutely. We have nowhere near the number of defenders we need to compare to the aggressive landscape we're in. I can only speak for New Zealand. I'm sure you can get the Australian figures. We have around 430 security professionals nationally. We have around 40 penetration testers, nationally. That's a tiny number.

We're a small country, admittedly, but that's nowhere near what we need. It can be a very demoralising state. Maybe I'm naïve or a bit broken or something, but I actually also think it's kind of exciting. Because while we do have those challenges, we're never going to have enough people to defend, it's a really amazing time to throw out the rule books and the old governance systems we're used to and go, "All right, if we haven't got much money and we don't have many people, then we can do other things."

We can innovate, we can automate so there's some beautiful opportunities here to embrace the new technologies that are coming through and apply them to security and make up for our lack of people.

David Pembroke: But that also goes to that original point, isn't it? Around that cultural change, and the key risks really are the simple things, and if you could just make a small impact in the behaviour of people around the basics, you're going to go a long way towards keeping yourself safe.

Laura Bell: Yeah, absolutely.

David Pembroke: What about this notion of skills? If it's not just around changing people's behaviour and those cultural elements, which are obviously important, those numbers that you outlined, even just in New Zealand, that sounds woefully nowhere near it, but how then do you see the industry developing in terms of getting people engaged in the learning, the training, the understanding, so as that you may double or even triple the number of defenders?

Not only in New Zealand, but globally, because I know exactly in Australia, same sort of problem, that there just are not enough cybersecurity professionals to deal with the challenge, and the scale of the challenge that everyone's facing at the moment.

Laura Bell: Well, what we're doing ourselves and what we're seeing echoed across the US and other places at this point is broadening who we consider is okay to be a security person. I love our community, so please friends who listen, don't be offended. I still love you. But we're very good at hiring people who look and sound exactly like us, who have the same background, who have the same qualifications, who went to the same schools, who work for the same employers.

At SafeStack, we have a team of roughly 14 at the moment. Now, we have on team a games developer, a reformed librarian; we have an illustrator and graphic designer. Not because, "Oh, my goodness, we were desperate and desperate times," but these were amazing people. In our interview process, we get people talking about how they would do harm. We get them thinking through scenarios and these people, regardless of their background, were amazing.

They were able to tell us how they would exploit systems, and more importantly, they were able to communicate how they would fix it. Communicators like graphic designers and illustrators have a gift that most of us security people don't have, in terms of getting messages across in easy to digest formats.

So, looking outside of our usual silos of just developers who went to security, or auditors who went to risk, we need to start going, "Well, how do we take the skills that were all in all sorts of groups of our population, and just add a little security on top?" That gives us a much more broad and diverse set of opinions and experiences and viewpoints, which is then fed into and shows in our approaches to security.

David Pembroke: So you're really reframing the challenge, aren't you? You're reframing the challenge as a way ... Going back to that point you raised earlier, around technology, that it's really not so much about the technology, it's about probably everything else.

Laura Bell: Yeah. We think as a company, it's just our opinion, that security companies are primarily communications companies. Our job is to translate very complex, different operating worlds, whether that's business or whether that's technology, and whether it's out in somewhere that's picking apples, and that's their business model, or if it's a giant high tech company.

Our job is to translate and communicate between these areas and help them understand how they can protect themselves. We are not magicians. We're not going to be the ones who come in and step in and fix their problems with some miracle solution, but we can help them understand their situation in a way that they haven't been naturally able to see themselves.

David Pembroke: Okay, that's really interesting. From a government point of view, what advice do you have to government information workers around what they need to know to be cyber aware and then what can they actually do to make sure that they're not contributing to what is obviously a very large and growing problem?

Laura Bell: So, for government workers particularly, there are a few things. Firstly, talk to each other. There are dozens of government departments in every country, and every country has a, particularly the ones that have a slightly British heritage along the way, we all this slightly siloed mentality where we'll have multiple departments doing similar things, but we don't cross-pollinate as often as we should.

Getting out there and sharing approaches and sharing challenges is a really important thing that we need to do way, way more of. The loudest voices in the room shouldn't always be paid security professionals like me. They should be the people who are in the trenches trying to do it themselves.

Furthermore, at least in this part of the world, there are quite heavy compliance frameworks around government agencies. We have rules to follow, we have reports to file, all of those kinds of things, and it's very tempting to feel like that routine, that audit cycle we go through every year is enough to save us. "The auditor will find it, and then we'll do our fixes, and then next year we'll be fine."

But we need to get out of that "Audit will save us" mentality, and start getting a little bit more hands-on. Not waiting for a control scheme to tell us what we should do, but really examining our own environments, and for each of the government departments out there, you each have a different set of data, which is interesting and valuable in different ways.

As we move to more open data and to more sharing, at the kind of data sharing and technology level, then that's going to become crucial, that we really understand the value that's specific to us, not just what the framework is valuing.

David Pembroke: It's interesting, isn't it? Because that sort of mirrors a lot of the emerging business processes and business practice, that you really do have to adopt this agile mindset at a time of digital transformation, 'cause it's not just in cyber, but I know in the focus that we have around the creation and curation and distribution of information, you have to again, adopt that same mentality, which is to basically run multiple experiments around what it is that you think is going to work for you.

Then measure the impact, and then adjust and adapt as a result of that. Really, it goes to this wider change, doesn't it? That we really have to think about the way we do our work differently, because we now live in a different world.

Laura Bell: Yeah, absolutely. In fact, there's a really interesting bit of psychology that plays into all of this, that we all need to be mind of. At SafeStack, we try to cross-pollinate between business psychology and understanding bias, and technology. We're a really hybrid mess of a group, but one of the things that we find really interesting is there's a rule in psychology that says, "The more something challenges your identity, the more it threatens what you're used to being measured as successful in, the more we will avoid doing it."

If you find that thing that you've had success in for 10 years, you've always done security this way, and everyone has always given you a good performance review, if you find that's being challenged, you might as an individual, very naturally try and defend it. But not in a way that's driven by any evidence, but just because it threatens the identity you have. We all need to be able to, if we're going to defend ourselves and each other, we have to be able to step back from that personal feeling and go, "Okay, let me see, can I justify it? Does it work?"

If we find that there's a gap, be open and brave enough to say, "Well actually, maybe we can do better" and try something new. There's a real risk if we let our own personal feelings and vulnerability get in the way, we'll never change the way we do things.

David Pembroke: It's a massive change, though, isn't it? That's a, as you say, if that's an underlying principle of most people and the way they manage their identity, and their self-worth and their value, that's going to be a big challenge, isn't it?

Laura Bell: It's huge. It's something we have to try and do together. This isn't going to be an overnight, we all read a self-help book, have a hug, and we all feel fine. But I think the more that security becomes a message that's cross, not just technology, but also talks about us as people, and why we're vulnerable and why this matters, the more people will be engaged with looking at themselves a little bit as part of that.

But it takes voices in all the right places to do that, so we need to make sure as an industry, that we're open and we're sharing.

David Pembroke: Fantastic. Well, listen Laura, thank you so much for giving up some of your time today, to speak to me and to the audience about this very relevant and important and critically important really, role that people play. 'Cause I think that's what I take from it, is that really this is a people job, more so than anything else. It's really those changing of mindsets that is going to really get us down the path to playing that role that we need to play to keep information safe, particularly those working in the public sector who own very, very valuable information and datasets around citizens, and so obviously that's information that needs to be held very securely, or as securely as possible.

Laura Bell: Absolutely.

David Pembroke: So thank you. Thanks for joining us, and thank you to the audience for coming back once again this week. Fascinating conversation there with Laura Bell, who is the CEO at SafeStack in New Zealand. Some wonderful, simple, clear, articulate, authentic advice, and things that we can employ in our day-to-day practice to ensure that we are doing the right thing. Thank you very much for coming back once again, and I will be back at the same time again next week, but for the moment, it's bye for now.

Speaker 1: You've been listening to InTransition, the program dedicated to the practice of content communication in the public sector. For most, visit us at contentgroup.com.au.