The Future of Cyber: Cybercrime

Featuring David Hickton as Interviewed by Bobbie Stempfley

Welcome to the SEI Podcast Series, a production of the Carnegie Mellon University Software Engineering Institute. The SEI is a federally funded research and development center sponsored by the U.S. Department of Defense. A transcript of today's podcast is posted on the SEI website at sei.cmu.edu/podcasts.

Bobbie Stempfley: Good afternoon. My name is Bobbie Stempfley. I am the director of the CERT Division at Carnegie Mellon University Software Engineering Institute, where we focus on cybersecurity and resilience.

My guest today is David Hickton. He is the director and founder of the University of Pittsburgh Institute for Cyber Law, Policy, and Security. He also has faculty appointments as professor in the [University of Pittsburgh] School of Law, the [University of Pittsburgh] School of Computing and Information, and the [University of Pittsburgh] Graduate School of Public and International Affairs. He previously served as the United States Attorney for the Western District of Pennsylvania, where he played a role in creating the legal practices for cyber-crime investigations.

I am really looking forward to our chat today. Thank you for joining us, Mr. Hickton.

David Hickton: Sure. Please, call me Dave.

Bobbie: My pleasure. The culture of computers and of information really has evolved so quickly. In our time together, it is just a completely different world today than it was 20, 10, even 5 years ago in so many instances. What I really like exploring is this idea of, *What are we going to face in the future?* and *How do we draw on what we have learned in the past?* and *How do we keep the pieces that are relevant and break with the pieces that aren't?* There is this tension between technology, law, policy, and regulation, and you have always lived at that tension point. Can you talk a little bit about the work you are doing today at the University of Pittsburgh?

David: Sure. Thank you. That really goes right to the sweet spot of why the Pitt Cyber Institute was created.

The gap between rapidly changing technology and very slow-moving laws and norms is growing every day. I like to tell people when I do my outreach or talk to my students, to just imagine the phones that you have gone through in the last five years. We used to think a flip phone was a technological advance, and now we consider it an artifice of a grandfather, and that is just a couple years ago. It has really gotten to the point where you can do everything on your personal device, and you don't really even need a hard portal in your office anymore.

This change has come upon us so rapidly, so fast. What we might envision in the future is probably beyond our imagination. Yet, the laws that we operate under, including the laws I used for the epic indictments that we did, really come from the Computer Fraud and Abuse Act of 1986. Just imagine, communication's change since then. What we are trying to do every day is answer the questions in that gap and be so bold as to say, as was true when I was in the government, *I wonder what Pittsburgh thinks?* We do that at Pitt. We do that in the partnership that exists every day between Pitt and CMU. It is a fantastic and very important partnership that has so many dimensions, and we try to create additional points of adhesion every day.

Bobbie: That gap is really fascinating to me, and in the places that [it] exists. You mentioned the indictments. It's really timely. We're recording this with [the] most recent indictments happening just yesterday. Take us back a little bit to 2014 when you indicted Chinese Army personnel for espionage. What did you learn from that, and how do you think it changed?

David: Well, that was a day, and even as we talk about the Equifax case, there is always going to be a paragraph in every story about every case since then, because the case that we did here in Pittsburgh on May 19, 2014, where we indicted five identifiable members, pictured members, of Unit 61398 of the People's Liberation Army of China, was the first case of its kind where the U.S. government used the tool of criminal indictment to stake out a legal position that we were no longer going to allow our intellectual property, our research, our innovation, our discoveries—which we protect here under our legal system—to be taken because someone could take them over the Internet.

My message at that time was theft is theft, and stealing is illegal around the world. This was really no different than someone pulling a truck up to a warehouse in the middle of the night and cracking the lock. It was just being done over the Internet. If you or I had done it, it would clearly and plainly be illegal, and we should just not accept it and not stand for it because the perpetrators were overseas. But that was a huge lift. That thought I had to get to that indictment was a huge lift. It was a multiple-year investigation. It really had been begging and coming for a decade before, before I was ever in the government. It required a complete metamorphosis, a complete change in perspective.

President Obama's executive order in 2011, which identified our intellectual property as a strategic asset, was my playbook. The support I had in the Eric Holder Justice Department to bring the case here was all the help I needed. We had the assets here in Pittsburgh. We had the will. We had the commitment, and we were either bold enough or stupid enough to believe that a case that could have fallen off the track at various points was worth doing with our little office of 50 lawyers here. It became the template for the Equifax case of yesterday, but we also did many more cases before I left the government at the end of 2016.

Bobbie: So, that template is, I think, really important. It had to have opened up any number of questions about how you approach cyber the same or different. You talked about it as theft is theft. I think a lot about this idea of attribution. Here at CMU and CERT we really think a lot about this. Some in the community have said attribution is a solved problem. Others have said it is not a solved problem. How do you think about that, and how did it shape your ability to indict?

David: Well, this is a dynamic challenge. It is not a static challenge, and it is going to continue to change because our adversaries have the advantage—whether they are individuals or nation-states—of hiding in the dark of the Internet. And, we have to play, *We got you. We caught you.* They are on offense. We are on defense. Every time that someone is hacked, there is a loss, and the cumulative effect of this has been described as the largest wealth transfer in human history. So, it really does matter. My view of it is that hacking can be complicated, or it can be simple. But, it is really attribution to defeat anonymization, and each of our adversaries has a signature. China has a huge, prolific army, and they do this in an open and obvious way. They sometimes mask what they are doing through hop points. In the case we did here in Pittsburgh, they used hop points of compromised computers in the United States, individuals and businesses, to mask the fact that these intrusions were coming from Shanghai in the middle of the night.

It appears in the Equifax case—I read the indictment yesterday—that they used hop points in Taiwan. The Chinese signature—using a large, open, and obvious campaign through some small measures of anonymization—is contrasted with the Russian signature, which is to have a bunch of subcontractors, criminals by day and perhaps government agents the rest of the day, and then to plausibly deny that they have control over them. North Korea and Iran, our other two principal adversaries, have different signatures as well, as has been reflected by the Cry, Cry Again and WannaCry attacks [See the SEI blog post on Distributed Denial of Service of Attacks: Four Best Practices for Prevention and Response], and then the Petya attacks, and some of the attacks on our government research by Iran, all of which go to core assets of our country. What was going on in my mind as I was doing it is, *Where are our children going to work? Where are we going to work, if we just surrender these assets?* It is just not acceptable to me to spend time talking about the difficulties of a new and involved campaign like that. You just start, and you go do it, and then you figure out later what the solution to the next fork in the road is.

One of the things that comes up every day—and it came up yesterday in Equifax—is the government acknowledges that these individuals are not likely to be brought to trial. But if you stop there, it is a defeatist attitude. In our case we did in 2014, everybody acknowledges that one year later President Xi in September 2015 made a deal with President Obama that said, *We understand that you are drawing the line on intellectual property, and we now get it. We are still going to spy on each other like we did in the pre-digital age, but we are not going to steal your intellectual property*. I think that it points to the fact that you need to take steps that outline what your laws and norms will be, and then you need to have a strategy for how that has collateral consequences.

All of my work, including that case and the case against Huawei, and the case against the Chinese fraud against our SAT system, and even a case here against an individual who was an on-the-ground spy, stealing PPG technology, that was just not accidental. It was a comprehensive plan by me, in organizing the assets I had here, for the purpose of not getting China, not being xenophobic, or not really even targeting China. It was really to bring law to digital space uniformly, so that the American citizens were not at a disadvantage when we had all the innovation. We had all the wealth. We were the largest economy in the world.

Bobbie: So that *bring law to digital space* I think is really an interesting lens to think about this. Because as I listen to you, it strikes me that one of the big changes in the last five or six years is really this appreciation of how we bring all elements of power into a dialogue around security, and the security of us physically, and the security of us economically, and the security of us digitally.

David: Right. It all starts with an investigation, and it starts with the dynamic concept of attribution, because you have to pin the cyber tail on the cyber donkey. If someone is intruding illegally, improperly into your system, you have to identify an IP address and tie it to that actor. Now whether you are going to bring an indictment, or you are going to bring a case in the Department of Treasury or the Department of Commerce or bring a trade case, you need that fundamental starting point of an investigation.

Bobbie: There is a technical component to that as well as a policy component.

David: Absolutely. Look, nobody does that better than the Pittsburgh FBI, but also nobody does it better than the Software Engineering Institute here at CMU, the CERT program here. These were assets that were identified, well before I was known in this area, as critical national assets. I said without challenge that virtually every case that was brought under my tenure, whether I signed the indictment or not, had a connection to Pittsburgh. We became a leader here because of the two universities principally and the FBI. Then it was up to me to identify this as a priority

and take the chance of putting almost my entire office on this with the prospect there would be no return.

Bobbie: One of the things that I think is a common theme through your career is this focus on the future and on, as you point out, how we think about the digital age. Two years ago, you chartered a Blue Ribbon Commission on Pennsylvania Election Security, and I had the privilege of joining you on the commission. Can you talk a little bit about the most important lessons you took from the commission's work about how to secure Pennsylvania voting?

David: It was a fascinating study. It was a great commission, and thank you for your service on it. I think, so far, it is the only real academic study commission.

Bobbie: I think so.

David: As we built it, it wasn't necessarily a lesson, but we understood that it had to be a representative commission to be effective. So, it was bipartisan. It was geographical. There was a blend of people like you and me who have served in government positions, but there were other people who have served in elected government positions on the state side. And, there were some people who dedicated their lives to voting from the League of Women Voters and Verified Voting.

So, we had a great commission. I was very blessed to have Paul McNulty co-chair it with me. Paul is a very distinguished college president now, but he had served as a U.S. attorney in the Bush Administration and then deputy attorney general: a very credentialed, very capable, a very good person. I think when you are going to do something like that, the most important thing is you don't start with your conclusion, and then decide how you are going to backfill. Enlightened people reason to their conclusion, and the challenge for leadership in a commission like that is to make sure that you actually do that.

The best example I can give your listeners of how that happened is, I wanted in the worst way, as you might imagine, as the leader in a cyber institute, to find a digital solution where we could protect voting on a digital platform the same way we protect our tax returns and our medical records. Everywhere I went I said, *Surely, there's got to be a way to do this*. As we just saw in Iowa in the Democratic caucuses, and we saw in Estonia, which we studied, and we saw with West Virginia, with service members who are overseas, it is just not the case. And I had to accept that.

My conclusion when I went in was, *We will find an answer here*. I tell your listeners now if there is someone out there who can find that answer, you will become very famous and very rich. Because we have to vote, and we can't abandon the digital platform, but right now the threats to the digital platform exceed our ability to protect it when it comes to voting.

Bobbie: The things highlighted in that report were really fascinating because it was really rich. Like most security and resilient situations, there is not a single thing that you can do. There are a slate of things that you have to pay attention to, as a part of it. And backup, recovery, audit are all an important part of the things that need to happen.

David: One thing I think, in retrospect, we did very well is we didn't try and take on the whole world or boil the ocean, if you will, on this. We did a Pennsylvania-specific project where we talked about machines, voting rules, and resiliency plans. That way we were able to put a manageable set of recommendations together. I think it was very, very helpful to the state of Pennsylvania, and my goal was to help the state of Pennsylvania be a leader, which I think we are.

Bobbie: That breakup also, I think, let other states select from the recommendations that are appropriate.

David: Right.

Bobbie: So, on the machine side there may be…In Pennsylvania there are guidelines issued by Pennsylvania law that may be the same or different in other states. And, on the rolls, how they think about that may be the same or different.

David: And we have 67 counties in Pennsylvania, and they were represented in our commission and presented as well. What you need in Philadelphia might be different than what you need in Potter County, and we accounted for that. But, we never tried to substitute our judgment for the discretion and vision of the decision makers. We just tried to be free labor with good ideas.

Bobbie: So, an incredibly complex situation, a socio-technical situation that I think...

David: It is. I feel very good about it, and I think that is the type of work we like to do.

Bobbie: So, let's talk a little bit about the technologies of the future and how you think about the landscape you have laid of investigations and where you think it needs to adjust as we talk about 5G, as we talk about artificial intelligence, as we talk about this hyperconnectivity that is there.

David: There are so many questions out there, that they just proliferate faster than we can answer them. But, the 5G question is a really important question. We need China. They are our number two economy in the world. They are going to, by size, pass us at some point. We can't isolate China. It is probably not a good idea strategically to get to the point that we have separate internets all over the world. One of the questions that was rich when I was U.S. attorney is, *Who owns the Internet?*

Now, we have this question of the Huawei 5G platform, which we have rejected but Great Britain has accepted, our top ally. *How do we manage that?* Every day, we have a question in the privacy arena. We were outrun by Europe with GDPR [General Data Protection Regulation]. They set forth in 2016 some privacy enhancements and then had the foresight to take two years to put them in place. When the most recent tech-lash occurred with regard to Facebook, you had the leaders of our tech companies saying that they were going to improve their game on privacy and adopt GDPR, which I think should be an awakening for us in America here, that we are sort of behind.

The whole concept of the privacy issue, the government versus these tech companies, we have a healthy skepticism of government in this country, and I understand that and respect it. The Boston Tea Party still resonates every day here. But it is paradoxical to me that the average American citizen is all ginned up about government intrusion, when we require here a warrant, probable cause, and a neutral judge, which is more than is required most places around the world. And, people regularly have their privacy breached by private tech companies who are not only eavesdropping on them, following their browsing patterns, and selling it for profit. That bill is before Congress right now. What are we going to do about that?

The whole issue of encryption is another one. It comes up every time we have one of these terror attacks. The San Bernardino terror attack was the first high-profile one. Now, we have had the Pensacola terror attack, where we have a dead terrorist and a locked phone. The question is, *What are we going to do about that?* I have said for a long time, if you just park that question in Pittsburgh, I could solve it, because people of good will can solve it if we get out of the Beltway. Because when it is discussed in the Beltway, you have these pejorative positions taken on both sides. One side says, *What if we have a 9-year-old girl who has one hour of oxygen left? Wouldn't you want to be able to breach that phone?* Then the other side says, *We must keep end-to-end encryption because it will, writ large, reduce hacking, and if you allow an exception, then the criminals will get in there first.*

Well, between those two extremes, there is an answer and people who are committed to answering it. We dealt with this before. We had the same question with trunks of cars and safes and pocketbooks and suitcases. Are we going to allow an inaccessible place where government action under our system dictates that there needs to be an intrusion for purposes of a case or for the greater good? I have asked the paradoxical question in my outreach, if we consider the fact that the entire highway of all of this information was paid for by the U.S. taxpayers through taxes that went to DARPA [Defense Advanced Research Projects Agency], which created the Internet. I mean let me give you this revelation. Al Gore did not create the Internet. It was created by the Defense Advanced Research Project Agency to facilitate the speed of communications for

defense researchers. Then we found it was so valuable, we put it for wide use. And, now it is everywhere.

We have effectively flown the plane to this point while we are building it. We have to answer these questions and more every single day. It is impossible for me to give you the entire landscape of what questions may exist, because I'm not prescient enough to understand where all this technology is going to go. I can only tell you that this concept of Moore's Law has been blown up, because it goes to the next level so fast that we can't keep up with it.

Bobbie: I think that question or that constantly seeking for what frameworks of the past apply, and then where we need to change those frameworks going forward, is really the thing that I see you constantly studying. It is not about throwing away what was in the past, because everything is new today, but it is about recognizing what is different and adapting or throwing away the parts that are necessary.

David: Yes, I am either stubborn or difficult. I think the thing that I deserve credit for is I just didn't accept things as they were presented to me. I had a blessing. I am not a career prosecutor, so I came to the U.S. Attorney's Office as a very credentialed lawyer, but I challenged everything, and I asked questions about everything. I think that is just a good way to live, because people get comfortable, and this is an area where you can't be comfortable. You have to become comfortable being uncomfortable here.

Bobbie: I think this is one of those places where you and I might approach these battles from slightly different perspectives, but the common ground is that I think we are constantly presented with false choices, and that we shouldn't accept that there are false choices. We should find the thing that we can do, and then focus on doing that.

David: Absolutely. Sometimes, the kinetic energy of the friction of an argument yields the answer. And, if you are unwilling to have that argument, you are never going to put enough heat to it.

Bobbie: As you pointed out, enlightened people reason to rational conclusions. So, thinking a lot about this idea of how we grow technical capacity for when an incident occurs, how do you think about what skills might be needed. We do a lot of workforce development activity for everything from cyber operators and forensics and other pieces. What are the skills gaps you see?

David: Back when I was U.S. attorney, I recognized that there was a big workforce development problem largely from the point of view that the FBI was training people, and then they would be hired by private industry. As I got to know it better, I have come to appreciate that the problem is much bigger than that. One of the first positions I accepted when I came to the University of Pittsburgh is I was asked to go on the board of CyberPatriot, which is an organization of the Air

Force Academy, where a huge priority for them is the cyber competition and a cyber camp to increase participation in STEM education, to create better opportunities for women in cyber, to create better opportunities for minorities. It is a wonderful on-ramp for a child of disadvantage to get a cyber training unit, because you can actually outrun your opportunity and almost catch up. Because the gap, we know, is several million people and growing, [the] gap being available cyber professionals and the need. I called for, in 2012, something which I think is sort of the seed of what I am doing today.

In a public speech, I called for the creation of the Pittsburgh Cyber Initiative, in a speech at the Community College of Allegheny County. That speech is still bouncing around somewhere on the Internet. But in that speech, I called for collaboration of our universities and a recognition that there are many places for people to find a job in cyber. You could work with machinery. There is a wonderful training center at the International Brotherhood of Electrical Workers here in Pittsburgh that people come from all over the world to see. So, if you are putting machines into place for the code writers to work on, you can be in the supply chain of the cyber platform that we are creating here.

Whether you go to high school, whether you go to trade school, whether you go to college or get a post-graduate education, there is a place for you in the cyber professions. I thought I was bold enough and provincial enough to believe that Pittsburgh ought to be the place that fills that need. We have always responded when the country had a need. We have historically been heroic in our response to that. We have the interest and the assets. Just earlier today you know that you and I were working together on trying to improve executive education in this area. I don't think we can do enough. I think it actually is a rich return for people who take advantage of these opportunities that we are going to create. It will make our region a place of destination for finding cyber professionals.

I will tell you that I was concerned when I was United States Attorney—I remain concerned today—about how we can take the necessary response, whether it is indictment or other, to the cyber threat and take it to scale, because the cases are so involved, and they are so long. What I was trying to do when I left the government is move them to other places where they could be litigated, if you will, in the government, other components of the government. I was trying to reduce the time of an investigation by creating a template. But of course, each investigation is different. As the cyber criminals change their tactics, you have to adjust as well.

I did training here for the Department of Justice, an immersion training program over two days, for 36 hours. It was very useful, where I brought in victims, people who were in our cases, and had them explain how hacking affects the lives of real people, which is critical. It was important that we did the case we did here in Pittsburgh in 2014, but it was almost of equal importance that we were able to identify the perpetrators and put their picture up, and the victims could be

identified, to tell the story. U.S. Steel was in that case. United Steelworkers, that was the spine of the case. But Westinghouse, Allegheny Technologies. There were other companies around the fringe that were involved. Alcoa was involved and Solar World, in the case, but there were other companies that were not named that were also victims of that.

By telling that story, it gave me the ability, when I would do my outreach, together with the PPG case I mentioned earlier, to tell this little vignette, especially when you put it in the context of theft of spots in our education system, in our public institutions. Imagine a Pittsburgh family, salt of the earth, people I grew up with when I went to high school here, and John and Jane Smith. Jane never went on to college, but was a secretary at PPG, and John was a foreman at U.S. Steel. And their most fervent hope, the American dream, was that they could provide a better life for their kids. So, Sally and Sam, their two kids, go to school, study hard, take the SAT the old-fashioned way. They actually show up and take it themselves, and they want to go to Pitt and Penn State.

The people they are competing against never took the SAT, because fictitious test takers took it for them, so that they could defraud the system and get a student visa and get access to spots in the entry class. At the same time that is going on, PPG has an engineer who is selling windshield technology to China, and U.S. Steel is being hacked mercilessly by Unit 61398, and it is causing plant closures and shutdowns and the decline of the Mon Valley. That is what it is. It is not just an antiseptic computer discussion about someone doing an unwanted intrusion in someone else's system. It affects real lives of real people. When we announced the cases, it was my mission to explain that, because I think that was lost until that happened. I think that was one of the great achievements of that case, because it creates awareness. The same thing can be said when you are talking about workforce development. If we don't come up with enough people to deal with this, to want to do this work and find it meaningful, we are going to fall behind in our ability to catch the threat.

Bobbie: It has been a theme of a number of my guests is this recognition that this is a socio-technical problem, not a technical problem. So, they really have to put a human narrative and a human face on all parts of this, of security and resilience, to get folks focused on it, to grow the workforce able to do it, and for folks to recognize the impact of it.

David: I would say that a little differently—and I want to say as a preface that I don't mean to criticize the importance of technical understanding of all things digital—but I say that it is a human behavior problem masquerading itself as a technical problem. Because we can never really catch up to the technology. The lag between our study and the change under Moore's Law is going to be disadvantageous to us forever. The change is going to be so rapid if we study that. What we can control, though, is human behavior. We can control law and policy, if we can lead, if we can use strategy, not buckshot, throw darts. If we can come up with a comprehensive plan

for how we are going to lead the world in developing new norms and new laws and understandings, and that is what I try to do today.

Bobbie: I think that is a gap in the way things had historically been, right? Folks recognizing where the technology might lead us to be able to understand the human behavioral element and how human behavior will both be adapted by the technology and can adapt the technology. I think those are...

David: And CyLab here does fantastic work on that already.

Bobbie: Absolutely. Lorrie was one of my guests, so it was really wonderful. Well, I really appreciate your coming and talking to us today. The challenges that your institute is facing and the opportunities we've had to collaborate have been really, really things I've treasured. So, I look forward to future opportunities.

David: Thank you. I appreciate you. I appreciate our friendship. I appreciate all the good work in the service and the government and the fine partnership that exists between the University of Pittsburgh and Carnegie Mellon University, which is one of the pillars of the strengths of this region.

Bobbie: I agree, I agree very much. If you would like to learn more about the University of Pittsburgh Institute of Cyber Law, Policy, and Security and what [it] is doing to close the gap between technology, law, and policy, please visit their website. To understand more about what we are doing at the CERT Division, and our role with helping with government, industry, and academia, please visit our website. Thank you.

Thanks for joining us. This episode is available where you download podcasts, including SoundCloud, Stitcher, TuneIn Radio, Google Podcasts, and Apple Podcasts. It is also available on the SEI website at sei.cmu.edu/podcasts and the SEI's YouTube channel. This copyrighted work is made available through the Software Engineering Institute, a federally funded research and development center sponsored by the U.S. Department of Defense. For more information about the SEI and this work, please visit www.sei.cmu.edu. As always, if you have any questions, please don't hesitate to email us at info@sei.cmu.edu. Thank you.