Unlocking the Secrets of Cybersecurity

Industry experts discuss the challenges of hacking, tracking, and attacking in a virtual world.

By Gil Klein

Shortly after Defense Secretary Leon Panetta warned of a “Cyber Pearl Harbor,” three of University of Maryland University College’s top advisers on cybersecurity agreed that he was wrong.

A cyber Pearl Harbor is not in our future, they said. It already happened—as long as 20 years ago. Sneak attacks against the nation’s computer infrastructure occur daily—from personal identity theft, to “hacktivists” trashing targeted Web sites, to thieves stealing corporate secrets, to foreign agents probing U.S. security weaknesses.

But with these dangers come opportunities. For people willing to get the right education, cybersecurity offers unlimited possibilities for creative employment that will provide essential services to the nation.

Speaking were three members of UMUC’s Cybersecurity Think Tank, which has helped the university establish undergraduate and graduate programs in cybersecurity education:

Retired U.S. Navy Rear Adm. Elizabeth Hight, who was vice director of the Defense Information Systems Agency and deputy director of JTF-Global Network Operations. She is now vice president of the Cybersecurity Solutions Group, U.S. Public Sector, of the Hewlett-Packard Co.

Marcus Sachs, vice president of national security policy at Verizon Communications, who coordinates cyber issues with federal, state, and local governments.

L. William Varner, president and chief operating officer of Mission, Cyber and Intelligence Solutions at ManTech International Corp.

They joined Achiever writer Gil Klein at the National Press Club in Washington, D.C., to probe this unprecedented new security threat. They talked about the possibility of what Panetta meant by a cyber Pearl Harbor—an overwhelming attack that shakes the nation’s security and economic system and warrants a military response.
A Pearl Harbor is usually painted as an unexpected attack, where the airplanes come in at dawn. Cyberspace is a little different. We’re constantly being attacked, we’re constantly being penetrated. So, many would say that our cyber Pearl Harbor moment is actually in our past. We just don’t recognize it. —MARCUS H. SACHS

But they were careful to emphasize that the situation is not totally dire. Solutions are available and opportunities abound to expand them to meet the ever-changing danger.

As Marcus Sachs said, “All is not bad. We may paint a very horrible picture here, but we want to make sure people understand it’s not the end of the world.”

GIL KLEIN: Betsy, what keeps you up at night?
ELIZABETH A. HIGHT: The whole host of “unknown unknowns,” whether they be very well-meaning but poorly educated information security officers, those who believe that the current host of products will keep their systems well defended, or those who have found unique and still undiscovered exploits to get into public, private, or personal systems. All of those things are still unknown unknowns to most of us.

GIL KLEIN: And Marc, do you sleep well?
MARCUS H. SACHS: Generally, I do, because if you know what bad is out there and what good is out there, you can sleep well. But what bothers a lot of people is that one lucky person. This is one of the problems in cyberspace: Somebody can make a mistake somewhere that we don’t know about, and somebody can get lucky—an unknown hacker, an unknown terrorist, an unknown criminal can get very lucky and do something very, very bad that’s unpredictable, and we only hear about it the next morning.

GIL KLEIN: And Bill, how about you?
L. WILLIAM VARNER: My real fear is the consequences of a successful cyber attack anywhere in our critical infrastructure.

I think we had a little taste last summer of what that might be like with the storms that came through the Washington, D.C., area. Many lost power for several days. I was fortunate to be able to find power sources nearby and keep my phone and laptop charged for the five days I was without power. But what would we have done had the power not come on in five days? What if it hadn’t come on for five weeks? I think our behavior as a society would change at that point, and it would be a much different place to live.

GIL KLEIN: Defense Secretary Leon Panetta, who probably doesn’t sleep at all given all his responsibilities, recently warned of a cyber Pearl Harbor. Now, let’s start with Marc. What do you think that would look like?
MARCUS H. SACHS: Well, fortunately, Pearl Harbor has already happened, and it probably happened about 20 years ago. The problem is that we don’t know what a Pearl Harbor looks like. When was the first intrusion into our networks? When was the first actual loss due to cyber crime? A Pearl Harbor is usually painted as an unexpected attack, where the airplanes come in at dawn.

Cyberspace is a little different. We’re constantly being attacked; we’re constantly being penetrated. So, many would say that our cyber Pearl Harbor moment is actually in our past. We just don’t recognize it. We’re still waiting for this big event, and we’re not paying attention to everything that has already happened.

ELIZABETH A. HIGHT: Most people equate Pearl Harbor with the Big Bang. I mean, there were bombs dropping, there were people injured and dying. There was a lot of noise. So when professionals use that reference, we think there’s going to be a great big, loud bang somewhere. But that’s not the way cyberspace works.

A BRIEF HISTORY OF CYBERSECURITY

BY MELISSA E. HATHAWAY, president of Hathaway Global Strategies and a member of UMUC’s Cyber Think Tank. Hathaway served in two presidential administrations, spearheading the Cyberspace Policy Review for President Barack Obama and leading the Comprehensive National Cybersecurity Initiative for President George W. Bush.

1969 ARPANet Transmission
1970 Intel introduces the first 1k DRAM chip
1971 Creepet Worm demonstrates mobility and self-replicating programs on ARPANet
1972 File Transfer and TCP
1973 ARPA Network Virtual Communication with Europe
1973 Motorola invents the first cellular portable telephone to be commercialized
1974 Development of the Graphical User Interface (GUI) paves the way for the intuitive design of Mac and Windows OS

Timeline content excerpted from a broader presentation and analysis.
So if we think about it that way, everyone will say, “Oh, no, no, there’ll never be a big Pearl Harbor.” But the consequences could be so severe that we would have exactly the same kind of mayhem, if in fact our critical infrastructure were destroyed or even penetrated in some way.

**L. WILLIAM VARNER:** And the worst thing is, we might not know until such an attack is well underway. It might not be the big, explosive, kinetic activity that we think we would immediately recognize.

**MARCUS H. SACHS:** It is, however, a fair analogy, because a lot of what led up to Pearl Harbor, what actually allowed it to happen, was the misinformation sharing and the stove-piping of information. People knew what was going on. We had intelligence, but there was no sharing. And this is exactly what we see today.

**GIL KLEIN:** And in general terms, how is the United States military preparing for a cyber attack? Is it happening quickly enough?

**L. WILLIAM VARNER:** We should look at the responsibilities of the U.S. Cyber Command and the Department of Homeland Security. Even more importantly, look at all of the aspects of our Internet infrastructure that are not protected by either the Cyber Command or Homeland Security.

What that means is that a lot of our protection today is left up to private industry. In all honesty, companies like ours are, in large measure, responsible for protecting their own networks.

And it’s a big challenge. The bad guys only have to be right once. We have to be right 100 percent of the time.

**GIL KLEIN:** Do you think the general public is aware of the threat? What more can be done to prepare the public for the possibility of a major cyber attack?

**MARCUS H. SACHS:** I think the awareness is there that cyberspace has problems. But what’s missing is the “So what?” What do I do about that? In the physical world, we do a pretty good job of teaching people about looking left and right before crossing the street or about not slipping on the ice. We don’t do as good a job of teaching people what to do in cyberspace to make themselves secure. That’s the education gap.

**ELIZABETH A. HIGHT:** People may be very aware of the threat, but they really don’t know how it impacts them personally. Unless they—or a close friend or family member—have had their identity stolen, for example, they won’t know the true impact on their credit report. They won’t know how long it will take to recover.
And when you’re at UMUC, or in any college environment, that is the time to take your innovative ideas and tinker with them and mature them. And then offer them to the greater good. Because cyberspace is open to all of us. So when you innovate, you’re helping all of us.

—ELIZABETH A. HIGHT

They won’t know that in fact what they put on social media is open to the world and will be there forever.

I tell people all the time that we need to have a cyberspace ethics and civics class in elementary school to help teach our citizens from the very beginning what this cyber thing is. Because children like to reach out and touch things, and they can’t do that in cyberspace.

GIL KLEIN: What is the need for a trained cybersecurity workforce? Are universities producing the numbers needed? Are there enough students coming out of high school with the skills needed to begin learning this kind of complex information? And, of course, how intense is the competition for these jobs? That’s a lot of questions.

L. WILLIAM VARNER: Those are easy questions, Gil, because the answer to most everything is no. There are not enough people currently. There are not enough people coming out of high schools or being trained in our colleges. And there are just not enough people in the general STEM—science, technology, engineering and math—curricula altogether.

I know Betsy and Marc and I all share an interest in trying to increase the number of trained cyber professionals in the country, particularly those who are able to obtain the clearances that let them work closely with our government agencies.

And we sponsor a lot of training programs. Just because someone graduates from college with a master’s degree in electrical engineering or computer science does not necessarily mean he or she is ready to join the ranks of cyber warriors.

MARCUS H. SACHS: Cyber education is a lot like health and health-care. When kids are going through elementary, middle, and high school, we teach basic health principles. But not all kids grow up to be doctors and nurses.

Cybersecurity is the same sort of thing. We need to teach the basics of hygiene in cyberspace, the basics of what can go wrong. Some can go on to become the professionals.

But I think what we’re missing is that early education. We tend to think this is only for the little geeks and wizards. But it should be for everybody, just like health education is for everybody.

ELIZABETH A. HIGHT: If ever there was a case for lifelong learning, it is cyberspace. All three of us are digital immigrants; we did not grow up with this technology. Our children and our grandchildren are very comfortable with it. But the technology is so complex and changes so rapidly, there is no one who can sit back and think, “Oh, well, I understand it, and I don’t need any more education.”

GIL KLEIN: Are there enough university programs to do this? Or is this an open field for universities? And who do you get to teach this if everybody knows it has to be working and protecting somebody?

MARCUS H. SACHS: There’s a lot of opportunity there.

L. WILLIAM VARNER: There is. UMUC has a great program. I also work with almost every university in the area, as well as with some that are not local. But to me, one of the most important things is making our career field attractive to people who are of the age where they are thinking about what kinds of careers they want.

MARCUS H. SACHS: It applies to all career fields. It’s not just for those who get a degree in cybersecurity. If your degree is in education, there needs to be a cybersecurity component, because you’re going to be the one talking to kids. You need to understand cyberspace at a level where you can talk about it, just like you talk about American history, just like you teach math.
But other career fields—engineering, law—are also wide open. It doesn’t just have to be focused on technical skills. I think this is where UMUC is really gaining an advantage, because they have a wide course curriculum, a big audience.

L. WILLIAM VARNER: And in the position we’re in now, I don’t think all of the universities and colleges added together could produce enough people to meet the needs that we have today.

GIL KLEIN: Talk a little bit about the kinds of attacks that are going on right now. Who is making these attacks? And how much impact do they have?

ELIZABETH A. HIGHT: There are basically three types of attackers. There are the hacktivists and the joyriders that we’ve seen for years and years. There are the state-sponsored attackers. And there are criminals. So each of them has varying degrees of support and education and training and opportunity.

That creates a huge problem for the entire federal, state, and local government environment, because they have to protect against the entire continuum.

MARCUS H. SACHS: There are some commonalities. It’s not machines that are attacking us; people are attacking us. The conversation we were just having about manpower—our adversaries have the same problem. There aren’t a lot of smart attackers out there, either. In fact, if I had the choice to work for one of us and have a beautiful, bright career, or to work for a terrorist organization and perhaps get blown up, I might decide that I don’t want to be a terrorist.

This is an interesting quandary, because our adversaries do face the same problems. Government targets are lucrative, but a government system is no different from a private sector system, or a university system, or a home system. It’s the same silicon, the same software, the same vulnerabilities.

The information may be different; the value of the information may be different, but that is actually a strength, because lessons that you learn in the government can be applied to industry, to academia, or to home systems. And vice versa.

So it’s a fairly level playing field in terms of defense. Solutions work in multiple places. And that’s a strength we need to play to.

GIL KLEIN: Can any of you tell me a story about an attack, how it came about, and what was accomplished?
MARCUS H. SACHS: What we see today usually comes on one of two levels. There is the subversive attack that is very hard to see. The adversary is interested in targeting you because there is information that they want specifically from you. And they will take time to get it. They go in and grab what they want, they take it, and you may not realize that it’s gone.

Often we see this happen after the fact. We have forensics teams that will go in and investigate, and a company or organization will realize that they have been breached. And it sometimes turns out that the initial entry was more than a year ago and the adversaries have had that much access before they are finally noticed.

Then you have the class of attacks that are very noisy, like denial-of-service attacks or flooding attacks. The target may be an organization like a bank or a government, or it may just be anybody who happens to be connected to the Internet. Those are like a flash; here today, gone a few moments later. But they can still be very visible.

And we face this all the time, particularly with high profile Web sites. This is the hacktivist problem we’re talking about, where in the past you might go up to whomever you didn’t like and spray paint your message all over their glass wall. Today, you go online and maybe deface their Web site, or cause a denial-of-service attack so their customers can’t get there.

ELIZABETH A. HIGHT: We’ve had cases of government organizations dealing with their own bureaucracies. A recent state case involved the lack of a state information security officer for more than a year. The thing that held it up was the bureaucracy of finding someone with these critical skills who would accept the pay of a person in a government bureaucracy.

Here in Washington, D.C., especially, I think the unemployment rate for cybersecurity specialists is less than zero. They’re in great demand. And that’s true not just for government but for industry as well.

GIL KLEIN: Bill, do you have a great story here?

L. WILLIAM VARNER: When you are attacked you might not even know it; the data is still there. They take a copy of it; they don’t take the data. It’s a lot different from physically breaking into a building and stealing something, where you notice, “Hey, my stereo system is gone.” You may not know that somebody has taken your valuable intellectual property.

MARCUS H. SACHS: Let me mention a real-world case here. The RSA Corporation, as many of us are aware, is at the top of their game when it comes to cybersecurity. Devices, software, consulting services, they’re all over. But yet they got breached.

And it kind of reflects back on that very first question: What keeps you up at night? Here you have the best, and they get broken into, even though they’re doing everything right.

ELIZABETH A. HIGHT: So 10, 15, or 20 years ago, we thought if we could protect the outer perimeter, we could keep all the bad guys out.

As a matter of fact, in 2005, the Department of Defense really cracked down on two-factor authentication and required everyone to log on to the network with their CAC cards—something that they knew, something that they held in their hands that could not be stolen by someone who was putting around in a network looking at the password file.

So those defenses were developed, and then we went on to phishing. And now we’re into spear phishing, and the human
element is so unpredictable. A very well-documented case that involved an effort to hack into an international company was really engineered around calling a system engineer overseas and claiming to be a member of the company. It was very late in the evening, and the system admin overseas said, “Sure, I can reset your password.” And the hacker actually got into the system that way.

GIL KLEIN: Is there a level of cyber attack that you think would warrant a traditional military response? Or could we even figure that out?

ELIZABETH A. HIGHT: I think with technology today, there are some who can figure that out. And as a citizen of the United States, if an organization or an individual actually turned off my power, or poisoned my water, or caused an airplane to crash, I certainly hope the United States would respond somehow.

MARCUS H. SACHS: That somehow is the question. Is the somehow diplomacy that ultimately finds its way into the military? Or is the somehow trade sanctions? Or is the somehow just a demarche or a public outing? I think that’s a public policy problem we have here in Washington. We don’t have that answer.

L. WILLIAM VARNER: Of course, that brings up the whole issue of attribution, which, in my opinion, is the most difficult problem in cybersecurity. You need to be pretty certain who launched the attack before you strike back. In reality, many attacks originate right here in the United States; they are just routed through other countries.

MARCUS H. SACHS: We have a very clear policy about the use of nuclear weapons, for example. There is no ambiguity about what the United States’ response would be if somebody fired a nuclear weapon at us. We have a very clear policy on invasion. But we don’t have a clear national policy that says, “It is the policy of the United States to do the following if there is a cyber attack that meets such-and-such a threshold.” I think we have to have that.
ELIZABETH A. HIGHT: And I think that is one of the great things about the UMUC curriculum. There are courses where students are challenged to think critically about those policy issues. And that area is ripe with opportunity, whether you’re a student, a private citizen, or a member of the legislative or judicial branch. Those discussions need to happen before we actually wake up one day and discover the catastrophic effect of a cyber attack.

L. WILLIAM VARNER: And the interesting thing we’re all saying here is that cyber technology is more advanced than cyber policy.

MARCUS H. SACHS: And of course cyberspace doesn’t belong to anybody. It belongs to everybody. It’s really a metaphor; it’s not really a thing. It’s not like dirt or air. It’s this made-up and synthetic thing that humans have built.

So when we ask the question, “What should the military do?” it really depends on whom you’re asking. Because a network owner and operator would say, “The military has no role here, other than perhaps protecting my physical assets. The actual essence of cyber-space is a business; it’s not a military battleground.”

So this is an ongoing debate here in Washington. Maybe we need to just keep talking about this, not wrapping it up behind classified doors, because it is a very serious policy matter that we have to start discussing openly.

ELIZABETH A. HIGHT: I think one of the things to consider is the foundation of our own country. I mean, individualism and privacy and all of those concepts that our country was founded on really fly in the face of cyberspace. Because a lot of people would say there is no privacy in cyberspace, and others would say that there is all kinds of privacy, it just depends on how you use cyberspace.

MARCUS H. SACHS: If you start with the Constitution, everybody understands the First Amendment. Freedom of speech, we want that; so, okay, we check that off. Then you get to the Second Amendment and things get very awkward. What does it mean to have the right to bear arms in cyberspace? What is an arm? And we’re only on the Second Amendment! We haven’t even gotten to Three or Four. [Laughter.] So, again, this is the debate we have got to have. What does this stuff mean?
GIL KLEIN: The United States and Israel apparently launched a successful cyber attack known as Stuxnet against Iran’s nuclear development program. Is that the type of low-level warfare we can expect to see that avoids actual firepower? Do you see an offensive use for the U.S. military?

ELIZABETH A. HIGHT: Well, I wouldn’t call trying to disable a country’s nuclear arsenal “low level.” I think that as we evolve in this arena, we will continue to see operations of certain types until we have case law or legislation that defines that.

I think one of the most important things to realize is that it’s not just U.S. citizens that are thinking about conducting defensive or offensive operations. This is a global domain; there is no state line or national border. And these conversations need to be held globally.

MARCUS H. SACHS: It’s hard for the United States because we’ve always been ahead of this game when it comes to technology—from airplanes to spaceships to nuclear weapons.

But enter cyberspace, and we just assume we’re in charge. We assume we have more capabilities than others. That may not be the case. And that’s very awkward for us, because now we have worthy adversaries. But they’re not necessarily countries like China or Russia. An adversary could be an individual, a corporation, a loosely affiliated group or a terrorist group. It could be a cause.

That’s what makes cyberspace so interesting. When we say what offensive is, we try to go back to our classic industrial thinking of tanks and planes and ships and invasions. But offensive in cyberspace may be completely different.

And I think Stuxnet is a great example, but it’s like a biplane compared to a strike fighter. This is so basic, to do a Stuxnet-type thing. And the history books will record this. Play this tape back even 10 years from now. Look at how we will refer to Stuxnet and say, “Wow, in its day that was pretty cool. But that’s so simple. We issue that capability to our kids; we show them how to do that to each other.” [Laughter.]

GIL KLEIN: So is this asymmetrical warfare taken to a new level?

L. WILLIAM VARNER: That’s an excellent question, because it is asymmetrical warfare, and the barriers to entry are small. They’re the cost of a laptop or a PC and an Internet subscription; that’s all it takes. It’s just an inordinate cost to defend against what an attacker can do almost for free.

MARCUS H. SACHS: But do you know the good news in all of this? There really are basic, simple things people can do to protect themselves. Oftentimes we do get wrapped up in the, “Oh dear, cyberspace is so dangerous; I think I’ll just unplug and go farm for the rest of my life.”

But it turns out there are a lot of very simple things that anybody can do to reasonably protect themselves, much like in the real world. We’ve learned that as humans and as part of society. I think that’s the piece that we’re hunting for with cyberspace: What are those basic things individuals can do? Because you’re always going to have threats, and you’re always going to have attackers.

GIL KLEIN: What is the responsibility of the private sector in providing a level of security? And what is the responsibility of the federal government in making sure that it is meeting that responsibility?

ELIZABETH A. HIGHT: I think cybersecurity has moved out of the computer operations center and into the boardroom. The boards and senior management teams who take the time to become educated in the risks associated with cybersecurity realize that there is a real reason to understand cybersecurity.

A wonderful SEC guidance came out recently saying that if you have a significant risk to a public company, it has to be reported, and that includes cyber risks. So I think that’s a step forward in educating both the boards and the senior management teams of industry.

MARCUS H. SACHS: Cybersecurity is now emerging as one of those areas where you’re actually better off if you’re outsourcing it and using what’s emerging as managed security services.

This has become so complex and so technical and so specific that it may be better as a business leader not to try to do it all yourself.

L. WILLIAM VARNER: This calls for a public/private partnership, along with a way to share information about attacks that may be
I use this phrase: “Hug an ethical hacker.” Start thinking about how to protect your systems by thinking like a bad guy.

One of the new industries that has sprung up is ethical hacking courses for senior government and industry executives.

—ELIZABETH A. HIGHT

ELIZABETH A. HIGHT: I think we have been talking about public/private partnerships for years. But in my view, most of these discussions are just far too general. They are not taken seriously by most people who are in control. Those individuals may like control, but they don’t understand that in fact they don’t have the expertise to keep up with this incredibly, remarkably dynamic, complex space.

GIL KLEIN: Along that line, former CIA Director James Woolsey said hackers are stealing us blind by breaking into company databases and taking secret development plans. How big a threat is this to U.S. business? And how adequate is the response?

MARCUS H. SACHS: Often when we say cyberspace, we really mean the Internet. But the Internet is just a piece of cyberspace. Air traffic control and interbank transfers don’t go over the Internet, for example, but they’re part of the communication infrastructure.

The Internet today is largely based on the explosion of personal computers back in the 1980s, followed by the explosion in the 1990s of the Internet itself, as everybody became familiar with it and as faster networks and laptops came along.

In the past five to 10 years, a new wave known as wireless has come along. We’re beginning to see a different type of device, different applications, different ways of thinking. And in fact, that wireless world is now bleeding into home security systems. It’s in your car, thanks to Bluetooth.

So there’s opportunity here. Where the old Internet is largely built on a string of wired PCs and hard drives, we now have a new cyberspace that’s coming out, largely Internet-centric, but with pieces that aren’t the Internet. And in fact, right behind that is this new thing called cloud computing.

So just like any other technology, we have waves of innovation. And what I think some are seeing is that each wave gives us the opportunity to add security that wasn’t there in the previous wave.

So cyberspace can in fact get more secure as we go forward. Just like any other technology, we have waves of innovation. And what I think some are seeing is that each wave gives us the opportunity to add security that wasn’t there in the previous wave.

So this is a well-recognized problem that academia, government, and private industry are all trying to solve.

GIL KLEIN: Is it possible to give an example?

L. WILLIAM VARNER: One estimate by people who are generally well regarded in the intelligence community is that at least one terabyte per day of U.S. intellectual property is being exfiltrated to other countries. So to put that in perspective, the written material in the Library of Congress comprises about 10 terabytes.

General Keith Alexander, the director of NSA and head of the U.S. Cyber Command, has stated publicly that he believes this is the largest wealth transfer in the history of the world.

ELIZABETH A. HIGHT: I think there’s a lot going on, both in government and industry. As a matter of fact, DARPA [the Defense Advanced Research Projects Agency] has recently released a fraud area announcement for some really exquisite defenses. And DARPA has hired some of the best-known hackers in the United States to turn their tradecraft into a defensive mechanism.

So this is a well-recognized problem that academia, government, and private industry are all trying to solve.

MARCUS H. SACHS: Often when we say cyberspace, we really mean the Internet. But the Internet is just a piece of cyberspace. Air traffic control and interbank transfers don’t go over the Internet, for example, but they’re part of the communication infrastructure.

The Internet today is largely based on the explosion of personal computers back in the 1980s, followed by the explosion in the 1990s of the Internet itself, as everybody became familiar with it and as faster networks and laptops came along.

In the past five to 10 years, a new wave known as wireless has come along. We’re beginning to see a different type of device, different applications, different ways of thinking. And in fact, that wireless world is now bleaching into home security systems. It’s in your car, thanks to Bluetooth.

So there’s opportunity here. Where the old Internet is largely built on a string of wired PCs and hard drives, we now have a new cyberspace that’s coming out, largely Internet-centric, but with pieces that aren’t the Internet. And in fact, right behind that is this new thing called cloud computing.

So just like any other technology, we have waves of innovation. And what I think some are seeing is that each wave gives us the opportunity to add security that wasn’t there in the previous wave.

So cyberspace can in fact get more secure as we go forward. Because we tend to build in new resiliency. We build in new safety features. We kind of build on previous mistakes.

continued on page 18
One estimate by people who are generally well regarded in the intelligence community is that at least one terabyte per day of U.S. intellectual property is being exfiltrated to other countries.

—L. WILLIAM VARNER

What I’m trying to say is that all is not bad. We may paint a very horrible picture here, but we want to make sure people understand it is not the end of the world. As new technologies come along, new vulnerabilities are introduced—don’t get me wrong there—but we are making some remarkable changes.

But for anybody who is interested in this area, the field is wide open for new ideas, new concepts. My company and your companies, we all have open doors for innovators, for new ideas, for fresh concepts and fresh ways of doing things.

And to kind of wrap this up, we’ve pushed the government right now not to regulate us, but to let us innovate. Let us find our way out of this security problem by being creative. That’s what Americans do best. We are the world’s best innovators.

ELIZABETH A. HIGHT: And when you’re at UMUC, or in any college environment, that is the time to take your innovative ideas and tinker with them and mature them. And then offer them to the greater good. Because cyberspace is open to all of us. So when you innovate, you’re helping all of us.

GIL KLEIN: So if you could get the ear of President Barack Obama or of Congress, what would you tell them?

MARCUS H. SACHS: If the president were sitting right here, I would like to know, first, what he does to protect himself as the leader of the most powerful nation in the world. What does he do personally in cyberspace? It may be a bit of an embarrassing question, because it catches a lot of people off guard: What do I do? Because I can pontificate all day long about what everybody else should do, but what do I do? That might lead to a very interesting discussion.

Now, the president might get it right, and might actually have a lot of insight. In which case, Mr. President, please stand up in front of the bully pulpit and start preaching. [Laughter.] But we don’t know where the president comes down on this.

ELIZABETH A. HIGHT: I think what you’re really saying is, “Be a role model.” That’s one of the barriers to getting our young people really excited about these careers.

I think it would be wonderful to shine a light on some of our heroes in cyberspace. And I think keeping everything behind the classified green door is a mistake.

I guess if I were across the table from the president, now that he has won a second term, I would say, “Take a chance. Look at the issues that need to be developed. Look at the lack of case law. Let’s think about what that means to our economic future and our personal privacy. Let’s look at those issues, now that you’re in a position to take that risk.” And I would say, “Go for it!”

L. WILLIAM VARNER: Right, so we would stress just exactly how important it is to develop that cybersecurity policy to the level of the policy and the doctrine we used to have, for example, in the days of the Cold War. We don’t have that for cyberspace.

GIL KLEIN: You mentioned cybersecurity heroes. Can you give me a case study or a story? Can you tell me a story about cybersecurity, or is it all still classified?

ELIZABETH A. HIGHT: Well, I know a lot of heroes who man network and security operations centers around the world for the United States military and for the Department of Homeland Security, and for some of our industry partners.

I know local and state government heroes that are doing that job every day. They’re sort of like firefighters and policemen. Until something terrible happens, you just don’t know about them.

GIL KLEIN: I was hoping you could give me a real name here.

MARCUS H. SACHS: There was a book called The Cuckoo’s Egg, by Cliff Stoll. Cliff was an astronomer in a university and recognized that there was a problem in one of his computing systems, where the accounting was off by a few pennies. Now, computers are precise. They should be exactly correct.

And when he found that they were off by a few pennies, he began to ask questions. Come to find out, there were intruders in there. And the intruders were changing the logs.

continued on page 20
But enter cyberspace, and we just assume we’re in charge. We assume we have more capabilities than others. That may not be the case. And that’s very awkward for us, because now we have worthy adversaries. But they’re not necessarily countries like China or Russia. An adversary could be an individual, a corporation, a loosely affiliated group or a terrorist group. It could be a cause.

—MARCUS H. SACHS

So an entire book has been written about this. It would make a fascinating movie.

GIL KLEIN: Bill, have you got any heroes out there?

L. WILLIAM VARNER: I think of some of the former directors of some of our major agencies—General Kenneth Minahan, for example, the former director of NSA [National Security Agency] and DIA [Defense Intelligence Agency]. He was involved in the very early beginnings of the Internet and working with Microsoft when some of the early vulnerabilities were discovered.

Bill Crowell is another cyber hero, I think. He’s now a venture capitalist, but he was a former deputy director of the NSA.

I think there are numerous people who have taken advantage of the positions that they had to make enormous strides in getting us to where we are today.

GIL KLEIN: Just to wrap up here, what I’m reading about is the next phase of the Internet; it’s so unbelievable, when you get into the cloud and you get into artificial intelligence. Do you see greater threats here? At some point you were saying, “No, this could actually be better for us.” We’ve come through 20 or so years of the Internet and the world’s still here. What are we doing right?

L. WILLIAM VARNER: In my opinion, Gil, we’re in a wonderful position. We have more technology than anybody ever dreamed we would have. We’re using it. My car sends me e-mails just to let me know how it’s doing.

And I do think we have the opportunity to make it even more secure, especially when we move into cloud environments. Because when the Internet was developed, security was just not a consideration; it was about communication and convenience.

We have tacitly made the assumption over all of these years that we value the convenience and the efficiency that we get from it. Web generations can build on what we’ve done?

But I think it’s a system that the entire world depends on. It would be very difficult to imagine living without it. So I think we’ve made tremendous strides, and we just have to continue to work very, very hard to deal with all the security issues that come up.

ELIZABETH A. HIGHT: This is a journey. A secure cyberspace is not necessarily a destination. With technology comes vulnerabilities. Our ability to recognize them is incredibly important.

I use this phrase: “Hug an ethical hacker.” Start thinking about how to protect your systems by thinking like a bad guy. One of the new industries that has sprung up is ethical hacking courses for senior government and industry executives.

This is a continuum that we will be on forever, long after we’re no longer here.

GIL KLEIN: Marc, do you have any final thoughts?

MARCUS H. SACHS: Cyberspace being a metaphor, it is also an extension of the human mind and human society, what we think and what we do. There’s opportunity for the bad guys to take advantage of it, and there’s opportunity for the good guys to do it right. And there are opportunities for governments, for the private sector, for academics.

Right now, we’re at the beginning of something really, really cool. And we’re the only generation that gets the first bite of the apple. Subsequent generations have to put up with our thinking.

When historians look back on our legacy, I hope they will say, “These guys got it right. Facing this complex challenge, they got it right.” Shame on us if hundreds of years from now they’re still fixing the problems that we come up with here.

I think that’s our challenge. That’s a challenge we can meet. But can we lead? Can we cause these changes so that future generations can build on what we’ve done?

GIL KLEIN: That is a terrific way to end this. Marc, Bill, and Betsy, thank you so much for being here. We certainly appreciate all the time you’ve given us. Thank you.

Google

Google announces new privacy policy

ISO/IEC 27032 publishes international guidelines on cybersecurity

Shamoon used against Saudi Aramco and damages some 30,000 computers (attack aimed at stopping oil and gas production at the biggest OPEC exporter)

Presidential Policy Directive 20 establishes national guidance for operations in cyberspace

Distributed Denial-of-Service against U.S. financial institutions peaks at 60 gigabytes/second

Hurricane Sandy affects power supplies and communication networks in northeastern U.S. for up to four weeks

U.S. Congress releases a report on national security issues posed by Chinese telecom companies

Syria shuts off Internet access across the country

World Conference on International Telecommunications (WCIT) updates and revises the International Telecommunication Regulations (ITR)