How Safe is Your Company?
Defending Your Company’s Assets in the Digital Wild West

Expert panelists at the San Diego Business Journal’s 2017 Cybersecurity Forum

The San Diego Business Journal hosted a Cybersecurity forum to an overflow crowd of business executives at the Paradise Point Resort & Spa on April 6. Today’s cybersecurity threats and defenses were explored by a panel of national experts in fields ranging from legal liabilities to cloud management. ESET Foundation’s Brad Lunn kicked off the forum and RADM (Ret) Kenneth Slaght of San Diego Cyber Center for Excellence moderated the panel discussion. Excerpts on the following pages were edited for brevity and clarity.

It’s Time to Design, Build IT Products With Security in Mind

Guest Speaker Brad Lunn of ESET Foundation set the tone for the day’s discussion, highlighting changing priorities that focus on product safety and security in an ever more threatening digital environment.

Product development: What’s changing is now we’re talking about products. We’re talking about products that are highly network enabled. We’re talking about products that are going to be used in consumer applications. We’re going to be talking about products that are in military applications. And the things that make us good at dealing with data center-centric type of cyber problems are not identical to protecting products. When you think about cybersecurity, we always talk about it from the risk standpoint, but there is also another angle to it. There is also an opportunity, and that opportunity is that since you know that your customers value security, they value safety; what if your product, your systems — one of the major dimensions of it was security.

When you think of IT organizations, good IT organizations, they are very good at dealing with technology, bringing technology in, utilizing technology, being users and consumers of technology. That’s different than what it takes to actually design, develop, deploy, support a product to be security-enabled from its foundation out into its product ecosystem, driving from requirements all the way through the engineering process.

If you’re in the space where you are building highly network-enabled products, you really need to be thinking it through from a standpoint of system engineering, of how are you going to design and build these products with security in mind from the start.

Finding Resources and Talent is Crucial for Cybersecurity Sector

We stood up three elements. The first one is a job board. It was a focal point where all the schools, colleges, transitioning veterans, all get access to the job boards. Then our members (including SPAWAR, 3,500 jobs a year in the San Diego region, almost half the workforce) could be posting their jobs. It is a huge disconnect, and it is all about communications.

We stood up three elements. The first one is a job board. It was a focal point where all the schools, colleges, transitioning veterans, all get access to the job boards. Then our members (including SPAWAR, 3,500 jobs a year in the San Diego region, almost half the workforce) could be posting their jobs. It is a huge disconnect, and it is all about communications.

We turned around to colleges and universities and said, “What are you guys doing? Why aren’t you growing? There is a huge demand signal for cyber talent in the region, and you’re not doing anything.” Of course, we should have done our homework. They were doing a lot, actually.

We found any jobs in cyber here in San Diego, so we’re going up to the Bay Area and back to Maryland.” Shame on us as a region. There is a huge disconnect, and it is all about communications.

Then the next, we worked with EDC and became part of their Linked2 program. If you want to get students aware of what is going on in the region, take your companies out to the universities, meet with the students who are interested in cyber, and make them aware of what is going on in the region.

But No. 3; you cannot just sit back and cross your arms and say, “Where is the talent?” Probably the most important element is we need to get serious about apprenticeships, internships, interaction with the universities, getting the students out in your companies to see what’s really available.
Eric Basu, CEO, Sentek Global Inc.

Eric Basu expanded on several key issues including the importance of an effective system, testing for weaknesses, evaluating IT vendor partners and our global disadvantage.

Cybersecurity’s relevance: The question is — why is cybersecurity relevant? It is back to the dynamics of humans, when one human had one thing and another human wanted to take it, the evaluation IT vendor partners and our effective system, testing for weaknesses, issues including the importance of an effective system, testing for weaknesses, and make that something μtual staffing, procedures and today's trust you attract talent when otherwise you don't have a firewall, it can often block out traffic. The code comes in, it calls back to home base, to the bad guy, say, what do I need to do now? I'm in this sys-tem, and it can block that as well. There are steps that you can take to prevent it happening. But obviously your last plan of good defense is backup recovery.

Security Should Be Viewed Through Risk Mitigation Lens

Stephen Cobb of ESET North America reviewed the importance of appropriate staffing, procedures and today's trust factor.

Effective staffing: I would say that building talent in-house is probably the preferred way in a lot of cases for smaller organizations and for organizations which are maybe on the periphery of the San Diego area that may not be able to attract talent as well as more urban areas.

In general, one of the problems I see is HR departments have not really learned yet how to hire for security. In many organizations, and this kind of surprised me, I typically work for very small com-panies, companies like myself, you don't have to be very large as a company for HR to come in between the people who are actually getting the employee and the people actually doing the work. We are seeing people really good programs now where four-year degrees are coming with some practical experience to it. I think that is an area that we can see something where the college going down this road — get them to do an internship. Work for a nonprofit for a while on helping them with their security, to find something under your belt in terms of what you have done in security.

One of the problems I've been studying for the past 12 months or so is the shortage of quality people to do cybersecurity for you. This is a very real problem, the cyber-security sales gap. There are at least, I think, 200,000 open positions that cannot be filled, not because they are not funded positions. These are funded positions that it is taking six months or more to find somebody for. And we see survey after survey on this problem. So if you are committed to security, you'll attract people who could go other places. They are going to come to you. If you take security on, and make that something you're committed to, it is going to help you attract talent when otherwise you might not be able to, because the right people are not the very, very top dollar. They are in it for the passion of doing the security right. And if you are paying a decent salary, and you are committed to security, you're going to have more quickly than you are doing it because it is very.

Distrusting technology: We're building our future and have predicted the future of our economy on digital technology, networked digital technology, and yet we are experiencing an erosion of trust in that technology which I fear will retard economic growth. ESET did a survey last October during Cybersecurity Awareness Month around the internet of things, and for the first time there were more than 50 percent of the people who said they were not thinking about purchasing a digital product because of concerns about security and privacy.

One of the biggest problems we're seeing at the moment is the lack of education. The lack of general knowledge of people about information sharing amongst governments and organizations, concerns about security and privacy.

For example, you ask them what the biggest trend last year and this year. And then, how much do I need? Do I need to spend a million dollars a year on backups to protect $500,000 worth of loss? Probably not.

Also, you need to have somebody from the government looking for you don't know what you don't know in terms of your IT. You have security people. They build in deliberate business vulnerabilities in there because of specific business reasons for doing that. For example, you ask them what the vulnerabilities are, they say, "we left this open so that we have to connect with the remote office." Vendor expertise and limitations: The problem is most IT vendors are not security specialists. That's the big one, you have to install their IT systems. They have not historically had an impetus to be security experts more than you have in terms of your daily operations. When you hire a security expert, you hire a guy who knows how to hack, somebody who is a CISSP, who goes to Black Hat every year, knows how to hack a little bit. What you are doing for the company is you are going to make your network built and make sure everybody has access to email. The IT vendors, they are doing the same thing. That's the reason why you're finding that your IT vendors actually don't know how to do it, and you should not expect somebody who is just an IT vendor to understand your security.

You think security is a distraction from your core business. If you don't do the security right, you may not have a core business, or it may impact your core business so significantly that your costs will increase, or you may not be able to stay in business anymore. You may not be profitable.

Ransomware is the biggest trend last year and this year.

Vulnerability assessment vs. pen test: You want me to do to now? I'm in this sys-

San Diego Business Journal

Security Should Be Viewed Through Risk Mitigation Lens

Eric Basu, CEO, Sentek Global Inc.

Eric Basu expanded on several key issues including the importance of an effective system, testing for weaknesses, evaluating IT vendor partners and our global disadvantage.

Cybersecurity’s relevance: The question is — why is cybersecurity relevant? It is back to the dynamics of humans, when one human had one thing and another human wanted to take it, the evaluation IT vendor partners and our effective system, testing for weaknesses, issues including the importance of an effective system, testing for weaknesses, and make that something μtual staffing, procedures and today's trust you attract talent when otherwise you don't have a firewall, it can often block out traffic. The code comes in, it calls back to home base, to the bad guy, say, what do I need to do now? I'm in this sys-tem, and it can block that as well. There are steps that you can take to prevent it happening. But obviously your last plan of good defense is backup recovery.
A data breach is inevitable. It is not a matter of if, it is a matter of when.

Are you 100% certain that your business’s critical information systems have never been compromised? If so, then read no further.

If you are not certain, or you don’t even know how to recognize a breach, then Sentek Cyber can help you.

Founded in San Diego 15 years ago, Sentek Cyber augments your current information systems and security staff with our outsourced Cyber Security Teams.

We start by helping you find unknown security gaps with our Vulnerability Assessments and Penetration Testing services.

Once you’ve identified those flaws, we will help you fix them and harden your defenses going forward using our Managed Security Services, in collaboration with partners including iBoss and AttackIQ. We can also help ensure that you meet all of your security compliance requirements with our PCI, HIPAA, and RMF audit teams. Our teams of “Sentekians” have an average of over 12 years of experience and are current on the latest techniques and exploits.

Let us help your company protect itself from cybersecurity threats.

---

SENTEK CYBER
A Division of Sentek Global

- Penetration Testing
- Vulnerability Assessments
- Cybersecurity Consultancy
- Advanced Threat Protection (ATP)

P. 619.300.9181 | www.sentekglobal.com/enterprise | info@sentekglobal.com
The Importance of Diligence, Monitoring and Vulnerability Testing

James Mapes, Director of Cyber Security Practice, TBConsulting

James Mapes of TBConsulting stressed the need for constant oversight and the results of human error.

Incident response plan: The way I was able to give some of our customers a litmus test was to ask, “Can you prevent a security event from becoming a full breach?” And if the answer to that question is, “I don’t know,” then you have some work ahead of you to do. Organizations that have realized that in the event of a breach, and as part of their incident response, they were going to need some outside resources. Typically IT departments are stretched thin and have some work ahead of you to do. Organizations that have realized that in the event of a breach, and as part of their incident response, they were going to need some outside resources. Typically IT departments are stretched thin and have another set of folks overwhelmed with this particular challenge. So being able to lean on a part of the team, the personnel that you need to to the know knowledge that you need to that incident.

But we’ve also been looking at making certain customers have table-topped an incident response plan and more importantly potentially included that as part of a pen test and it is a great means by which to have some fun, with some of your teams in doing red team, blue team, letting them go at it against each other. It is definitely important to test that you’ll be surprised at some of the things you thought you had that, in fact, you don’t. You don’t want to be finding that out when you are in the middle of an incident.

Human error: No amount of technology, no amount of hardening can prepare you for human stupidity. So it is really important that companies start thinking beyond just that first layer of security. It is important they are able to engage in the business. They need to be able to see information security is a business issue first and foremost. You can say, okay, the big problem is what is at or is causing the issues here, but it is a business problem that needs to be solved.

And get educated. One of the reasons I bring that up is you may have a solid group of IT folks that may be very interested in information security, and the cost of a few courses for them to come up to speed is a hell of a lot less than what incident response will be for you in the long run.

Due diligence: There are a lot of people who own businesses, who own technology and don’t know how to use it and how it is used in their business. I think it is important to come up to speed for that, because that is essentially the weapon you’ll have to defend yourself. That is important, because there is no law enforcement out there right now who will protect you from the attackers that will attack you.

On a proactive basis I recommend you get away from the idea you can get by with an annual vulnerability assessment and an annual pen test. These are things you need to be doing all the time. You should be doing them monthly if not to a point where it can be as much as on a vulnerability side, running some sort of vulnerability management program in-house. The reason you want to do that is you want to discover what your vulnerabilities are. Obviously, the next thing you want to do from a proactive basis is mitigate them or remediate them, and that is very important, because it is those vulnerabilities that will get you compromised. So if you take the proactive response of reducing them, you reduce the number of changes out there to compromise.

It is extremely important here. Knowing yourself and knowing your weaknesses, that is your pen test and your vulnerability assessments. The next thing to know is who is coming after you — what data you have and what value it has to somebody. It is very important to take a look at what you believe is your threat profile. Once you have that information, you can be pretty well armed to come up with a good program.

Businesses today, organizations today, have to essentially be secure a hundred percent of the time, and your adversary only has to get lucky once, and they’re in. It is incredibly unfair, and the chances are that you are going to have an incident.

Don’t Become Complacent with Cloud-based Services and Compliance

Chris Orlando, Co-founder & CSMO, ScaleMatrix

Chris Orlando of ScaleMatrix spoke on where our cloud technology is today and the importance of compliance.

Utilizing the cloud: We come at things from the data center and cloud and service center perspective. We see a lot of folks overwhelmed with this particular challenge. So being able to lean on a partner for that is something that provides a layered approach. You have another set of eyes that help you with the day-to-day to make sure not only are the boxes checked, but there is a way to enforce it. We are trying to help the folks have a 24/7 viewpoint of things. We find there is a little bit of complacency taking place in this cloud-enabled world where we are about abstracting the hardware layer and the operational pieces, managing servers and infrastructures, and just going back to focusing on applications.

From a financial standpoint while we’re asked to spend more today, the cost of storing data has gone down dramatically, and the function of the platforms that are supported are improving greatly. We have regional availability centers. You back up something to one center once, and we have service so you’ve got multiple connections and it is punch button simple.

In our world, the data centers get spread out. They are no longer the individual locations. We are pushing content closer to the edge, closer to the eyeball, and with that we are spreading out connectivity to millions and millions, if not billions of devices and having a clear and concise way of securing communication. And something we don’t use is a great handle on yet, but it is becoming more and more what we have to do.

Many of our cloud customers, folks in the Bitcoining business, folks in the analytics business, folks in the data platform business, go to block chain as a service and are using it to help improve operational fortitude around data protection. That is something we are seeing starting to take effect and being a larger piece of the business profile.

Compliance: You will see a lot of common themes we are talking about today. For us, we preach a lot about going back to the basics for compliance and all the efforts we go through from a security perspective, it is a check box for a lot of folks. If you operationalize that and use it as a training media and start getting people involved in the process and actually work those things, you provide at least that base layer so you are not a complete and total open target for everybody that is out there.

We live, eat, and breathe operational fortitude. That is part of what we do from a compliance perspective. In our world you have to do it. It is part of a prerequisite to be a player in that business...

Businesses today, organizations today, have to essentially be secure a hundred percent of the time, and your adversary only has to get lucky once, and they’re in. It is incredibly unfair, and the chances are that you are going to have an incident.

We live, eat, and breathe operational fortitude. That is part of what we do from a compliance perspective. In our world you have to do it. It is part of a prerequisite to be a player in that business...
DO MORE FOR YOUR BUSINESS

Keep your data, devices and employees protected with IT security software from ESET.

ESET.COM/US/BUSINESS
Protecting Your Company from the Outside and the Inside

Justine Phillips, Special Counsel, Sheppard Mullin

Justine Phillips of Sheppard Mullin spoke about recent trending threats, the importance of insurance protection, proper budgeting for the correct services, and the critical need to prioritize security in internal company cultures.

Current threats: Things that have been keeping me up lately are ransomware attacks, phishing for W-2 and wire transfers. Spoofed email accounts have been a real problem. The less fun part is seeing the fallout and the very real business consequences that happen as a result of some of these preventable attacks. The first two quarters of the year for W-2 attacks is really high. Those are January to around April and May, because they want us to take that data and submit tax returns on behalf of all of the employees.

Another current issue today is the M&A process. Cyber diligence and figuring out whether or not your intellectual property that you are trying to sell for hundreds of millions of dollars has already been breached and is being made somewhere else for a lot cheaper. So that is a huge issue. If you have any hope to sell a company, just be thinking about that.

Contracts, insurance and indemnification: Take a look at those agreements you have with vendors who may be housing your data or transmitting or accessing your system. Look for two things: Look for an indemnity provision, and see if it indicates who is going to be on the hook when it is a breach of your client or employee data; and number two is ask them to be an additional insured on their insurance policy. They will have great insurance coverage. It costs you nothing, and I have been seeing an uptick in companies who have been allowing that.

You also can be liable for a vendor error. So make sure anytime you are providing sensitive information, it has a social security number that is encrypted along with payroll information that has employee information in combination with date of birth. Anytime you are providing information out or you are allowing access in, make sure those agreements with those vendors are solid. Make sure there is indemnity. It is really clear. Maybe they have an instant response plan. Ask to see theirs. Maybe adopt theirs.

Part of the problem is we don’t have a single rule of law that governs all personally identifiable information. That is a state-by-state analysis. And if you are maintaining data on folks in all 50 states, then you have to comply with those regulations and laws in all 50 states. That’s very difficult for companies.

Insurance is a great risk mitigation tool. If you go through the application process of a cyber policy, you’ll remediate a lot of the risks and problems, because they ask you the right questions. They ask you: Do you have an instant response plan? What type of data are you maintaining? How many consumer records do you have? It is a great checklist to walk through with your key stakeholders who know the answers.

Budgeting and prioritizing security: My best advice to give, as a starting point, is to convene that cyber committee within your organization. Go through the checklist, whether it is an insurance policy or some other checklist, and start doing a cost benefit analysis. It might not make sense to do monthly vulnerability scans or pen tests, but it might make sense to at least know what your baseline is if you have never done it.

Understanding what data you have, and really starting to have conversations such as do we need insurance? Can we afford insurance? Let’s talk about our broker. Have monthly meetings, bring in lunch, know and educate your fellow co-workers around the subject of cyber. I think a lot of things flow from that.

And when you start having those conversations with the right stakeholders in the room, from the top down, you need the information security people, HR people on policies. You need to understand who your team is going to be. You need to have the controller or somebody from finance, because you’re going to ultimately need money. But you need to understand at the end of the day what is going to ruin your business if it is breached, and how can you look at security as more than just a cost center.

A lot of businesses have so many things to be spending money on. And security is one of those. How important is it? Is it going to ruin my business if I’m breached? I think most people have a fixed mindset in thinking, “I don’t understand it.”

I see part of the problem being the inability for people who are not computer-minded or literate thinking that anything related to a computer must be the computer guy’s job, and they have got security because I have no idea what I’m doing or talking about. I also don’t see a lot of vendors accepting accountability and responsibility for their own deficiencies in being proactive and telling folks, “Hey, this is not something that I really do.”

Training your employees is your greatest line of defense as well as the culture we were talking about, “Hey, we don’t want you to click on the dancing cat. The dancing cat is bad. We know it is funny, but please don’t do that.” Or developing some policies that say you can’t check your personal email from your workstation, or you can’t have a BYOD connecting to our system unless you have certain security protocols in place.
Aligning IT With Your Business

Technical Business Consulting—TBC—is your business partner that helps you achieve 100% alignment of your technology with your business objectives.

Partnership with TB Consulting offers a variety of benefits.

Thought Leadership
We partner with our clients by understanding their business needs, and bringing the right technologies to address their challenges.

Partnership
Your needs are significant and diverse. We embrace the pace of change, and aim to exceed your expectations with focus on the outcome, not just contract terms.

Structured
ITIL based practices regarding Strategy, Design, Governance, Implementation and Operations ensure that risk is managed by utilizing best practices.

Honesty
We welcome feedback and communicate honestly. We don’t hide from challenges.

Savings
TBC aggregates demand amongst all of our clients and invests in industry leading solutions (Gartner Magic Quadrant) with meaningful savings passed along to you.

Our partnership mentality drives all of our decisions.

Here’s our commitment to you:

We do the right thing at all times, focusing on your needs before our own.

We own and resolve your issues, even if it’s “not our job.”

We seek ways to drive costs down while increasing capabilities.

We invest in you to show our commitment as your partner.

Contact TB Consulting today to get started
602.263.8921
defensive capabilities. But, as individual citizens we have zero ability to do any kind of defensibility without running afoul of our law enforcement.

This is not the case in China. You are not going to be a Chinese citizen and go hack the Chinese government. You are not going to last very long if you do that. But if you have any kind of skills, the Chinese government is going to recruit you.

In Russia you have the combination of the oligarchs, organized crime, and the Russian government. They are all in cahoots. The Russian government doesn’t care if the Russian criminal organizations are happening. They love the fact that this is a breeding ground for them to develop.

We are trying to develop our defense systems on the up-and-up over here with the universities and other things and keeping people on the clean side of the law. So in those we are behind them. It doesn’t mean we aren’t going to pass them up as America does in many, many cases, but they are not bound by the rule of law the way we are. So when it comes to doing criminal acts, they are perfectly happy to let their citizens do criminal acts and then recruit them. They will find the best hackers and bring them to the government.

No point pricing or application fee
Appraisal cost credited back at closing
Up to 30-year amortization and 10-year term

Call a SDCCU’ commercial lending specialist for today’s low rates!
Marc Mathews, Vice President
(877) 732-2848, ext. 4616

It’s not big bank banking. It’s better™

sdccu.com/business
(877) 732-2848, ext. 5200

San Diego County
Credit Union®

REALTIME REPORTING
Our team of Nationally Certified
Realtime Reporters stands ready to
meet your legal transcription needs.

WORLDWIDE COVERAGE
From San Francisco to Taipei, we
provide our best-in-class court
reporting anywhere in the world.

TECHNOLOGY
Power up your next case with live
video streaming, videoconferencing
and video synchronization.

CASE MANAGEMENT
Instant access to transcripts, exhibits,
calendar and more. Available 24/7
online and with our mobile app.
WHAT WOULD YOU DO IF YOUR COMPANY’S DATA WAS HACKED OR COMPROMISED?

Does your business have the right level of protection in place to ensure it would survive such an attack? Here are some necessary steps we can suggest to help protect against these situations.

3-2-1 Principle
2 copies of your data stored on 2 different media types and 1 offline copy.

Move to the Cloud
It’s cost effective, your data is always secure and accessible in real time.

Test Often
Simulate real-world data loss scenarios by testing internally and often.

SCALE MATRIX

VEEAM
CLOUD & SERVICE PROVIDER
PLATINUM

FIRST MONTH FREE
scalematrix.com/veeam
(858)633-4300
sales@scalematrix.com
A packed room of close to 200 business executives heard experts from the multifaceted world of cybersecurity at San Diego Business Journal forum. The event, part of an ongoing popular series, was held on Thursday, April 6, at Paradise Point Resort & Spa. The morning featured insights into the latest threats and most effective defenses available for businesses in the ever changing digital arena.

Support for the forum included title sponsor Cox Business, gold sponsors ESET North America, ScaleMatrix, Sentek Global Inc., TBConsulting; table sponsor Proficio; and in association with the Cyber Center of Excellence.
1. Rod Weiss, Coleman University; Armon Mills, Publisher Emeritus, San Diego Business Journal
2. David Davis, Victor Holguin, both with Business Complete Solutions
4. Kevin Bostenero, Pat Nunally, Russell Packer, Fred Falk, all with e. Digital Corp.; Victor Rivera, Gold Sponsor ScaleMatrix
5. Joe Rubio, Damon Moore, both with Blue Nose IT Solution Inc.; Jonas Litonjua, WW Grainger
6. Jamie Valdez, Buffini and Company; Steve Croll, Gold Sponsor ScaleMatrix; Josh Mazur, Carlsbad Chamber of Commerce
7. Donna Kruse, Teleproviders; Panelist James Mapes, Steve Walker, Eric MacWan, KJ Song, Joe DiBiase, Scott Laughlin, all with Gold Sponsor TBConsulting
8. Kaitlin Jones, Kimberly Scholz, both with Table Sponsor Profinco
9. Oscar Peralta, Jason Laughhead, both with Title Sponsor Cox Business; Randy Hurt, GotUWired
10. Brandon Gunter, Moss Adams LLP
11. Ian Whitman, Rosano Partners; Dan Adams, Wells Fargo
12. Alex Hosch, San Diego Metropolitan Credit Union
13. Philip Baddour, Scripps Laboratories; Bruce Mayberry, Maxine Price, Central San Diego Black Chamber of Commerce; Angel Mason, Puzzle Pieces Marketing
14. Liane Monaco-Christensen, University of Phoenix; EJ Conrad, Island Staffing
16. Amy Wimer, Associate Publisher, San Diego Business Journal; Todd Backus, Title Sponsor Cox Business
17. Cheryl Soto, Josh Franklin, Franklin | Soto LLP

Photos by Bob Thompson, Fotowerks. Additional photos from the event are at the following link: http://fotowerks.sdbj.smugmug.com.