A Guidacent Special Report:

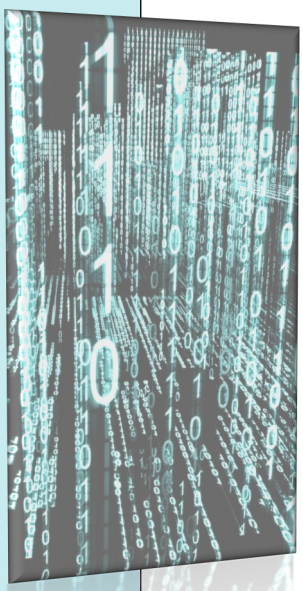
Guidacent®
Program Leadership & Innovation

How At Risk Is Your Company?

What Every Executive Should Know About Data Security and Risk

It starts with a short, but ominous phone call from someone on your leadership team, *"I think we might have an issue, a few customers have alerted accounting about services they paid for but never received…we're trying to find out what's going on…"*

"How many customers…and how much were the services?"



"Sounds like 25 or 30…and one was over $23,000. I'm not sure how far it goes yet...but I've asked security to look into it for answers..."

"Answers? What should we even be asking them?"

As a "non-security" executive, what questions are you going to ask? What should you understand about data security, your risk, and your level of preparedness? This special report will help to equip you with the questions to ask, and provide key insights from data security experts on steps you should take to manage and control your level of risk.

For the past few years, we at Guidacent, a Seattle-based business and technology consulting firm, have been hearing a growing number of concerns and questions from our clients related to data security, especially with so many high-profile breaches in the news. Many of these concerns were voiced by executives not closely involved with technology or security, but who needed to know their company's plans and levels of risk.

...hearing a growing number of concerns and questions from our clients related to data security, especially with so many high-profile breaches in the news.

To help our clients and others learn more about data security, and what questions they should be asking of their security people, we put together a roundtable event featuring a panel of two prominent security executives, **Sean Murphy**, CISO with Premera Blue Cross and **Chuck Markarian,** CISO at PACCAR, along with moderator, **Jason Robinett**, Guidacent senior consultant and security expert.

Guidacent roundtable events are designed to be small, intimate events, where the experts can share their thoughts and participants can ask questions and get direct feedback.

Prior to the event, we assembled a series of questions to ask our panelists, then took a few additional questions from the audience. We hope you'll find the questions and especially the answers, to be of value for your organization. Our thanks to Jason, Sean, and Chuck, as well as those in attendance for making this a most fruitful discussion, and pleasant evening.

Jason: "First of all, thank you both for being here. Let's hop right into it...what would you say are the key ideas or concepts you believe these executives should know and take back to their organizations about security?"

Sean: "I would say security awareness and training. 65-80% of all data breaches start with human error and come from within an organization. Having employees know what do to and how to handle information in the right way is really important. Another one is company culture. If the company culture does not support security, than it's not going to be important. Finally, I'd say to realize that security isn't a technology issue. You should reframe security into a risk conversation. At the end of the day, your systems may be secure, but you still need to manage risk and quantify it; define acceptable risks."

"...65-80% of all data breaches start with human error."

Chuck: "Similarly education and also patch maintenance. When it comes to security, employees are a company's weakest link; most of security issues, by far, start with phishing — an employee clicking on a malware link. So train your employees. Test them with phishing emails, understand what's going on with security, get involved. It doesn't matter if you're a small or large company. If money is involved, you'll be a target. Finally I would say, patch your systems. Many companies fall behind on patch maintenance and it's critical to stay on top of it."

"Understand your metrics for patching; your goal should be 95-100%."

Jason: "So let's say something happens, someone gets into your systems, what do you do on the back-end?"

Chuck: "First of all, you should have an attitude that you are, at some point, going to get breached, and you need to have an organizational plan ready with your response. Especially a plan for how to identify and repair your most sensitive data. But before that happens, make sure you're doing all you can to keep intruders out, like protecting your home; you lock the doors, alarm the house, do all you can to keep the nosy people out. If you get good at the basics like patching, monitoring, hardening systems, you can help keep the nosy people out of your systems ."

Sean: "I agree. Have a defensive approach, and realize that keeping all security threats away entirely will be impossible. You must improve your detection and response plans, and they have to begin in hours, not days. Security issues are compounded when they are found through an audit or you are notified by your customers. An incident response plan is a plan that you should have now! And make sure you have a business response plan as well as a technology response plan. Don't build it when you need it."

Jason: "Something many people are talking about is GDPR, General Data Protection Regulation, adopted by the EU a few years back. It seems to be the new buzz word in security. Is there a cheat sheet, or some things executives should be thinking about regarding GDPR?

Chuck: "Europe has stringent privacy laws; all entities in Europe must have GDPR in place. The fines are substantial and the key date everyone needs to focus on is May 25, 2018."

Sean: "For healthcare, this could be the next Y2K, and I'd say go to the IAPP – International Association of Privacy Professionals for guidelines for more information"

iapp
international association of privacy professionals

Jason: "Let's talk about the questions company boards ask you and the challenges you address with them"

Sean: "There's a range of questions; some boards will just come out and ask, 'What should we be asking you?' Not many boards have a cybersecurity seat on their board. Then of course you get, 'What are we doing to be secure?' and 'Do you have everything that you need?'"

Chuck: "They ask, 'How do we compare to our peers?' There are some companies that can benchmark their security, so they'll want to know about our progression, and are we doing what we need to do? They'll also ask about the security roadmap and execution of it. One challenge they need to think about, is do we have too much security, and could we be causing our own problem. My suggestion is to be cautious, but move quickly."

Jason: "How can you measure ROI on security investments?"

Chuck: "It's hard to quantify, but if you have controls in place, you'll get a return on your investment."

Sean: "I agree it's hard to show. I think IT will have a tough time communicating ROI, but good security enables business functions, it can help with competitive advantage. Of course having trust with your customers is a big thing. Some of you may have heard about cybersecurity insurance, where if you have a data breach, there are now underwriting policies that you can purchase."

ROI? "...**good security enables business functions, it can help with competitive advantage. Of course having trust with your customers is a big thing.**"

Jason: "Speaking of investment, can you benchmark how much an organization should spend on security programs?"

Sean: "For healthcare, security can be 2-10% of an IT budget."

Chuck: "I've typically seen security fall under the IT budget. For the manufacturing space, the IT budget is 2 – 4% of a company's revenue. Security is typically a small portion of that, but that portion is increasing."

Jason: "Two recent vulnerabilities are Spectre and Meltdown...What is your take on them? Do we need to worry?"

Sean: "I'd say focus on patching. Do what you can to control things, even though exploits haven't been seen yet. At the end of the day, it's still takes a vulnerable system to be exploited."

Chuck: "It's real; there's a lot of hype about how it may impact every device. Make sure patches are up to date, and isolate systems as much as you can."

"So let's assume the worst, you have a breach… what do you do?"

Jason: "Okay...from a business and communications point of view, what do you do? How broadly do you communicate?"

Sean: "Make sure you have an issue, then walk through your incident response plan. If you don't have one, have an outside incident response firm put one together for you now. You'll get a breach, so plan for it. Also, call the FBI – they are focused on finding the perpetrator. Finally, have an internal crisis management team. Own the issue, take care of your customers and do it on a timeline that's reasonable. Don't hide."

Chuck: "I'd add to practice, make sure you run through scenarios. You should never be the panicked guy, show that it's under control to portray a good sense of trust."

Jason: "How do you get non-technical people involved in security?"
Sean: "Security awareness and training. Have a security liaison, a security point of contact. Have someone be the ambassador for security in your group."

Chuck: "Have a security deputy, and invite your security rep to your department meetings."

Jason: "What does security awareness and training look like?"
Chuck: "It needs to be really engaging, put together skits or videos so it gets their attention, do video conferencing. You could conduct brown bags, and do your own phishing, but don't make it punitive so you can measure it."

Sean: "It's more of a process than a thing. Have annual requirements. When hiring an employee, have security be in the intro packet. Do ad hoc training on current events. Quick team meetings for 5 minutes and bring life to the content."

Check-List For What To Do WHEN (Not if) a Breach Happens:

- **Make sure you have an issue**
- **Walk through your incident response plan (so HAVE ONE)**
- **Call the FBI**
- **Have an internal crises management team**
- **Own the issue, take care of your customers...don't hide**
- **Practice, do mock scenarios**
- **Don't panic...show that it's all under control**

What You Will Learn In This Special Report:

1) **Key concepts every non-security executive should know and be asking about related to cyber security and risk.**
2) **Benchmarks for investing in data security and how to measure ROI.**
3) **How to put a plan in place before a data breach happens (and it WILL happen to every company at some point).**
4) **Immediate steps to take once you suspect a breach has happened.**
5) **What data security training should look like and who should be included?**

Guidacent roundtable events are designed to bring together thought leaders and industry experts to provide helpful insights and suggestions.

Our Roundtable Event Panel of Experts:

Sean Murphy
CISO, Premera

Sean Murphy is a proven healthcare information privacy and security leader and board-certified senior-level healthcare executive with Premera. He is considered the pro's pro for privacy and security management, DIACAP, HIPAA, FISMA, PCI, Meaningful Use, and OCR preparation and audits. Sean is the author of "Healthcare Information Security and Privacy."

Chuck Markarian
CISO, PACCAR

Chuck Markarian is accountable for all elements of Information Security globally, across all PACCAR divisions. This includes security consulting, investigations, litigation support, strategic planning, and standards. Chuck has two security certifications from ISACA (Information Systems Audit and Control Association); CISM (Certified in Information Security Management) and CRISC (Certified in Risk and Information Systems Controls).

Moderated by Jason Robinett

Guidacent Senior Consultant and Security Expert

The Guidacent Transformational Roundtables 2018

April 19, 2018
Agile Transformation

July 19, 2018
Cloud Transformation

October 25, 2018
Guidacent Networking Mixer
Fun event for clients and guests

Our Events Fill Quickly, Please Contact Greg Bennett For Early Registration!

Greg.Bennett@Guidacent.com

Guidacent®
Program Leadership & Innovation

Your success is our top priority. We have seasoned experts focused on delivering outcomes.

About Guidacent
Guidacent is a consulting firm leading the way for companies to achieve their most crucial IT and business goals.

425.943.6112
www.Guidacent.com