Guidacent®

Guidacent Business Brief

Data Integrity:
Where IT Hurts
(7 Important Questions)

Guidacent®

Guidacent® secureD@ta

Data Integrity: Where IT Hurts

(7 Important Questions)

da♦ta *(noun)*

1. individual facts, statistics, or items of information, often numeric.

2. a set of values of qualitative or quantitative variables about one or more persons or objects.

You ARE at Risk ... and it starts with a short, but ominous phone call from one of the managers within your operation: "I think we might have an issue. Our customers have alerted accounting about services they paid for but never received. We're trying to find out what's going on …"

A Data Compromise means trouble. Data Integrity refers to the overall accuracy, completeness, and consistency of data.

Businesses are becoming more vulnerable to cyber threats due to the increasing reliance on distributed and remote computing environments, programs, and social media.

Data breaches, which include the most common cyber attacks, pose an existential threat and potentially devastating impact on businesses of all sizes. These breaches frequently arise from gaps in security controls or processes that have not been fully implemented.

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, Guidacent has been hearing a growing number of concerns and questions from our clients related to data integrity, 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.

Guidacent®

DATA INTEGRITY

*To help our clients and others gain a better, more informed understanding of data security, and seven relevant issues they should be asking of their security people, we assembled a moderated panel discussion involving three cybersecurity executives, **Sean Murphy**, CISO with Boeing Employee Federal Credit Union, **Chuck Markarian**, CISO at PACCAR Automotive, and **Drew Williams**, Cybersecurity Practice Director at **Guidacent**.*

Why it Matters

- 75-80% of all data breaches are due to **Human Error**
- Any business should make it a goal of patching their **100%** of their systems
- 92% of all malware attacks connect through **eMail**

Guidacent® secureD@ta

Moderator: ***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, 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."

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."

Drew: "I agree that security awareness is the foundation where it all starts, but targeting that awareness is critical. The world of 'cybersecurity' is intimidating and tends to be filled with ambiguity and fluctuations. Executives often don't know what to really focus on—I often refer to it as herding birds. So, focusing those awareness programs on **specific topics** will definitely impact the security posture of any organization. So, focusing on Passwords, Phishing and Access should be at the core of any awareness efforts"

Guidacent®

DATA INTEGRITY

Guidacent® secureD@ta

Moderator: ***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."

Want to Improve Data Integrity?

- **Multi-factor Authentication**
- **Strong, Complex Passwords**
- **System Patches & Updates**

Drew: "It still surprises me at the number of businesses that think so carefully about advancing their goals but forget about the elements of risk when something goes wrong.

"A solid business recovery plan is essential to making sure everybody knows what to do when the lights go off. And they WILL go off at some point.

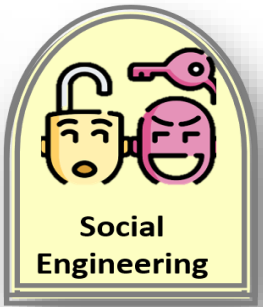
"But that doesn't mean everyone needs to go into 'Panic' mode. That's why table-top exercises are so valuable."

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."

One of the oldest, best used threats to everyone is that email or text message that warns of an account needing updating



Social Engineering can happen from anywhere—including phone calls, on-site visits, or even from behind a customer service desk

One of the fastest things everyone can do to impact their security is by keeping strong passwords for all of their accounts. It's as easy as 1-2-3-4!

In a post-pandemic world, many businesses have adopted the remote "work from home" model. But how do they stay secure?

DATA INTEGRITY

Moderator: *"Let's talk 'Data Privacy.' There's a lot of buzz about the European GDPR data protection rules, and the subsequent California CCPA. It seems to be the new buzz word in security."*

Chuck: "Europe has stringent privacy laws; all entities in Europe must have GDPR in place. The fines are substantial."

Drew: "Data privacy is going to take a big turn on regulation. We are seeing more and more states adopt mandates—mostly based on the GDPR and subsequent CCPA. This will continue to be an issue."

Sean: "For example, in 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.

Sean Murphy is a former healthcare information privacy and security executive and board-certified senior level healthcare professional now serving as CISO for BECU. Sean is the author of "Healthcare Information Security and Privacy.

Chuck Markarian (CISM, CRISC), is the Chief Information Security Officer for all PACCAR divisions. His responsibilities include security investigations, litigation support, strategic planning, and standards.

Drew Williams' 42-year history in Information Management & Security began with his time in Navy Public Affairs. Drew launched one of the IT Security industry's first Host Intrusion Detection systems (HIDS), an early SIEM, and one of the first Security Services/Hacker Research teams (Symantec SWAT Team).

Moderator: *"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.

Drew: "We are seeing something of an evolution in the cycle. A few years back it was all about selling the whole "Fear works" campaign. Then it went back to ROI, and now we're seeing a new trend emerge: "ROSI" or Return on *Security* Investment. And I agree, the Cyber insurance is an excellent way to go, especially if you're concerned about the growing trend of Ransomware attacks."

Moderator: *"From a business and information 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."

Chuck: "Own the issue, take care of your customers and do it on a timeline that's reasonable. Don't hide. And never become that guy who panics. Show that it's under control to portray a good sense of trust."

Guidacent®

Guidacent® secureD@ta

Moderator: ***"How do non-technical people focus on improving Data Integrity?"***

Sean: "Security awareness and training. Have a security liaison, a security point of contact. Have someone be the ambassador for security in your group."

Drew: "Take the fear out of it. Explain things in basic terms that everyone can understand and actually relate to. Nothing says, "I don't care" like throwing a bunch of acronyms at a group of people and expecting them to want to understand what they mean."

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

Moderator: ***"What does Security Awareness Training look like?"***

Drew: "It's got to be something that will keep people's attention and interest, so it needs to be a series of brief, relevant, interesting, timely and interactive engagements—either online, in person or through some multimedia means. But security is only part of the solution.

Chuck: "Security Awareness Training 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 five minutes and bring life to the content."

*Here are **5 Quick Wins** any business can do immediately to reduce the risk of loss from a cyber attack:*

1. *Ensure **Passwords** are complex and don't contain personal information.*
2. *Activate any Multi Factor **Authentication** features that are available.*
3. *System **Updates** throughout your entire business is critical for system integrity.*
4. *Keep "Cybersecurity" at the forefront of your **training** and awareness efforts.*
5. *Check your security **posture** on a regular basis to ensure your processes still work.*

Ready to learn how Guidacent can help your business **improve** its ability to keep your **Data** Secure?

Email us at **info@Guidacent.com** to schedule a free consultation.