ACHIEVING DATA-CENTRIC SECURITY

How Commodity Traders Can Fend Off Breaches by Being Brilliant at the Basics
INTRODUCTION

The increasingly digitized and connected world of commodities trading is experiencing ever-growing cyber risk as the threat surface expands both inside and outside the organization.

Increasingly, cyber attacks are planned and executed with targeted criminal intent. The commodities industry is under concerted attack from criminals and hacktivists with the dual objectives of causing financial and reputational damage.

While the chief information security officer (CISO) manages an organization’s response to cybersecurity, it should be a priority for the whole business. As such, it requires cross-organizational collaboration. The business should manage cybersecurity risk with the same rigor and accountability as more traditional commercial and operational risks, working together to identify and respond to growing threats.

Businesses need to understand their overall cybersecurity profile and develop a comprehensive cybersecurity strategy to help mitigate their cyber risk. With many companies failing to recognize that cybersecurity is an issue in the first place, what is the best way to proceed?

In commodities trading, successful defense requires that traders effectively practice cybersecurity fundamentals. Responsibility falls across the organization, but direction and prioritization start at the top. Ensuring the basics are followed and their effectiveness measured is the foundation of a successful cyber defense strategy.
THE COMMODITIES INDUSTRY IS UNDER ATTACK

Information technology (IT) in commodities trading commonly suffers from lack of investment. That makes the industry vulnerable to threats due to aging infrastructure and applications—and attractive to attackers because of the high value of typical transactions. For example, a recent NotPetya attack on a container shipping company resulted in the shutdown of its port terminals, resulting in US$300 million in total costs.¹

In another example, a grain trader’s systems were subject to an attack that left it infected with a virus. The company was unable to connect to its regular information system and had to resort to manual processes. Traders were unable to trade. The malware slowed wheat and fertilizer shipments and threatened to impact the flow of soybeans to the country’s main client, China, at the height of export season.²

These are not isolated incidents. They reveal a common truth: The risks would have been much lower if the organizations involved had effectively practiced the basics of data-centric security. Now more than ever, every organization serious about protecting its data must review and implement data-centric security fundamentals.
KEY TAKEAWAYS

Data breaches are incredibly costly
Estimates put financial losses of a severe event into the tens or even hundreds of millions of US dollars. Beyond that is damage to brand and reputation and ongoing financial and legal exposure. Research independently conducted by the Ponemon Institute and jointly developed by Accenture estimates that the cost of cyber crime is now 23 percent more than last year, costing companies US$11.7 million on average.3

Organizations suffering breaches have not fully appreciated the value of data as the lifeblood of business
In commodities, compromised data may put human safety at risk in the physical supply chain. Yet it is more likely to lead to competitive disadvantage, damage to brand and reputation, and significant legal and financial consequences.

Trading depends on relationships, and despite recent technology advances, these relationships have always been based on trust. The interconnectedness, volume and velocity of transactions today have made digital trust a vital concern. Would you want to deal with an insecure counterparty that might offer an insecure gateway into your own data?

In the digital era of transparent markets, data is value. Those who guard that value have significant advantage over those who do not.
Organizations that suffer data breaches typically have multiple points of failure

The issue is not the attack method. Whether criminal attackers exploited a known vulnerability the targeted organization failed to patch or launched a zero-day attack, the result is the same. The real issue is that multiple processes and procedures had to fail for organizations to be exfiltrated—and for that exfiltration to sometimes go undetected for days, weeks or months.

All of this adds up to straightforward, prescriptive advice: The commodity industry needs to get its data protection fundamentals in order. To fend off and minimize the impact of data breaches, now is the time to “harden” data assets and make it an organizational priority to practice data-centric security basics.

**ACTIONS**

**Effective cyber defense depends on doing these basics well. Check if you can identify the approaches employed within your own organization. If anything is missing, it may be time to reassess your strategy.**

1. **IDENTIFY YOUR HIGH-VALUE ASSETS**

These are your “crown jewels”—the data most critical to the business, subject to the most stringent regulatory penalties and most important to your trading edge and differentiation in the market.
2. HARDEN YOUR HIGH-VALUE ASSETS

“Hardening” high-value assets means making it as difficult and costly as possible for adversaries to achieve their goals. Hardening also limits the damage attackers can cause if they do obtain access:

- Adopt the attacker’s mindset. What do they want most? Design and execute your threat and vulnerability program, and overall security solution, to deny it.

- Consider and use multiple techniques—including encryption, tokenization, micro-segmentation, privilege and digital rights management, selective redaction and data scrambling.

- If your high-value assets are on legacy systems, don’t try to harden those assets all at once. Instead, increase protection and visibility over control points or points of access until you migrate or modernize the legacy systems. If you have legacy systems that can’t be suitably hardened, look for opportunities to restrict access and upgrade your monitoring. Be laser-focused on timely detection at your weakest links.

- Remember that with all the focus on securing data—encrypting it, keeping it in the safest of systems—if the same controls are not applied to people who have access to the data, you have simply moved the point of failure. To fully protect your high-value assets, keep “the people dimension” in mind.
3. **BUILD UP YOUR DEFENSES THROUGH NETWORK ENCLAVES**

Your company is no longer securing only a well-defined perimeter. Required protection now extends well beyond your “four walls” to include physical counterparties, banking partners, joint venture partners and even the companies that fill your vending machine or maintain your air conditioning.

Consider creating enclaves, which limit an attacker’s maneuverability. These environments both on and off premises enable you to better monitor the comings and goings of users and the behavior of applications. When the perimeter is breached, the enclaves remain safe. Think of a ship. If the hull is breached, maintaining independent watertight bulkheads will prevent the ship from sinking. In the same way, hard-partitioned enclaves in your network prevent a breach from moving laterally through the entire enterprise.

4. **BUILD AND EXECUTE A HUNTING PROGRAM**

There was a time when organizations felt they only had to activate their incident response plans in the event of a breach. Not any longer. Today, the best approach is to adopt a continuous response model. In other words, always assume you have been breached. Use your incident response and threat hunting teams to always look for the next breach. Above all, find them before they find you.

5. **BUILD AND USE ADVERSARY SIMULATION AND CATASTROPHE SCENARIOS**

Run and test those scenarios for end-to-end effectiveness to verify and validate that you can detect an adversary, and that your people are prepared and ready.
6. SCAN YOUR APPLICATIONS

Scanning is important because it helps identify actual vulnerabilities—ideally as soon as they are discovered and reported. However, it is only one component in an overall security framework. To optimize scanning efforts, have as complete a grasp as possible on your external assets. Know what you need to scan, who owns the assets and who can fix vulnerabilities. Make sure your security team can validate scanning results and quickly eliminate false positives. Integrate security into the software development cycle, so you can address bugs more cost-effectively before scanning. Measure the resolution time for vulnerabilities and help the business prioritize remediating those that pose the greatest risk. Application scanning is not just having a tool but rather having a robust end-to-end program to decrease security risk in a cost-effective manner.

7. PATCH YOUR SYSTEMS

Organizations fail to patch their systems because they have a fluid system landscape. They may not know how many systems are active in their inventory. If they do have an inventory, they might not know all the different versions of software on their platforms. A patch to a certain version of an operating system might break the application on top of it. A threat intelligence program can provide automatic notification when specific applications with high-value assets require a patch to avoid being exploited. The program must also reconcile anomalies, such as a patch that requires a reboot on a system prohibited from rebooting.
8. **LIMIT, MONITOR AND SEGMENT ACCESS**

Use two-factor authentication as much as possible, and use role-based access to automate decisions about who is allowed to see what data and systems. Move toward micro-segmentation in your access control, recognizing that when sensitive data needs to be adjudicated by different people for different reasons, none may need to see the data in totality. Micro-segmentation can show each person what he or she needs to see based on his or her roles and responsibilities, while obscuring the rest. This also limits damage in the event of a breach—if any one user’s credentials are compromised, only a portion of the data is exposed. To exfiltrate whole objects or larger sets of data, the adversary’s job becomes much more difficult.

9. **MONITOR FOR ANOMALOUS AND SUSPICIOUS ACTIVITY**

Monitor continuously and vigilantly not just for unauthorized access but also for undiscovered threats and suspicious user behavior.

10. **DEVELOP BOTH STRATEGIC AND TACTICAL THREAT INTELLIGENCE**

Have a sustainable threat intelligence program that collects and curates both strategic and tactical threat intelligence. Strategic threat intelligence is human intelligence coming from a variety of both closed and open sources. Other forms of strategic intelligence can provide insights on campaigns targeting certain industries or technologies, or geopolitical trends that could change the incentives of attackers. Tactical threat intelligence includes machine indicators of compromise that feed in automatically to your systems. Stay as current as possible on both the broader threat landscape and the specific threats posed by adversaries as they relate to your organization.
11. **BUILD A SECURITY ECOSYSTEM**

Traditional introspection and reliance on in-house solutions is no longer sufficient. The threat landscape is moving so fast that internal talent and skills need to be supplemented with a diverse specialist support system. When necessary and appropriate, take advantage of the assistance that managed services organizations can deliver to access capabilities quickly and economically.

12. **PREPARE FOR THE WORST**

Transform your incident response plan into a crisis management plan that can be enacted if the worst-case scenario materializes. Make sure legal and corporate communications teams are on “stand by” and prepared to take action. Exercise the plan so that the business builds muscle memory and identifies areas for improvement before the next issue arises. Be ready for a catastrophic cyber-attack where email, voice over IP and other communication systems used on a day-to-day basis are unavailable. For such catastrophes, consider storing critical contact information in the cloud and being prepared to use the cloud as a secondary platform for email and voice communication.
CONCLUSION

Too often, talk of cybersecurity prompts business eyes to glaze over—and then gaze over to IT. But remember: Your digital door is already open. Adopting a “pass the buck” attitude is ultimately an invitation to hackers.

Cybersecurity threats are evolving day by day. They represent a real risk and should be managed as rigorously and comprehensively as any other commercial risk. That depends on having the right direction from business leadership, developing a comprehensive approach to cyber defense and embedding the responsibility for effective cybersecurity throughout the company as a cultural norm.

The cybersecurity threat is not existential. It is here now. It is pervasive. If you ignore it or unthinkingly delegate it, it is simply a matter of time before your business is impacted. When security and risk leaders make cybersecurity “business relevant,” the cyber-committed CEO and board of directors become engaged, not just involved. The time is now to be proactive and work together to protect the commodities trading industry.
References


Contact Us

Richard Payne
Managing Director – Commodities Trading & Risk Management
richard.payne@accenture.com

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world’s largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 425,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.