BUSINESS ANALYTICS

Protecting the Brand Jewels

Machine Learning and Advanced Analytics Drive Effective Cybersecurity and Risk Management

Coauthored By:
Dan Woods, CITO Research
Charles Griffith, Teradata Corporation

In *The Cuckoo's Egg*, Cliff Stoll follows an obscure accounting discrepancy and discovers that hackers breached his company's systems. Stoll's story is a parable for enterprise security in our modern age: As it turns out, paying close attention to what is normal and what is not is key to cybersecurity and risk management alike. These days, machine learning and advanced analytics are used to investigate the types of anomalies that Stoll found, abnormalities that indicate a problem.

The processes being used in cybersecurity can guide strategy for risk management for businesses of all sizes. By applying the lessons of cybersecurity, it is possible to achieve the goal of risk management, which is to identify and prevent the maximum risks for the least amount of money.

To do this, companies must take a portfolio approach to risk management, while also accepting two baseline facts:

① **Money can't buy security. You can never be risk free:** No amount of spending can make a company completely secure. The challenge is to find ways to detect and prevent both likely and unexpected problems while focusing on the challenges that pose the greatest risks to your business.

② **People are the problem and the solution:** The people in an organization are the easiest targets and the greatest assets for detecting and managing risks. Creating a culture that prioritizes security, devoting resources to training and awareness, and ensuring compliance with policies is a task that is starts with C-level executives.

Just like Kubler-Ross's model of grief, it's easy to deny these hard truths. But accepting them lays the foundation for building a system that will get you the most protection for the money.

Why a portfolio approach to cybersecurity is needed

Modern cybersecurity acknowledges that it's not possible to build an impenetrable fortress.

We should do everything we can to prevent attacks. But we also need to recognize our fortifications will fail, and when they do, we need to have a failsafe in place.

For example, adding layers of protection, using strong encryption, help ensure that if attackers break in, they actually get nothing in return.

The best way to address the complex problem of cybersecurity, as pointed out in "Why Most IT Security Suffers from Unbalanced Spending," is through a portfolio approach. Here are some of the steps in threat detection that are being supported using machine learning and advanced analytics:

- **Define normal:** Use behavior and big data to create a sophisticated definition of normal activity.
- **Flag abnormalities:** Monitor your system constantly and use machine learning and advanced analytics to identify flag events that seem strange.
- **Prioritize the crown jewels:** Put extra layers of protection (encryption) on the most important information. Threats to your most important information dangerous should receive immediate attention.
- **Press stop:** Once problems are identified, implement a manual or automatic way to halt the attack, counteract it, and re-secure operations.

As covered in "How to Choose the Right Eyes and Ears for Cybersecurity," there are a wide variety of solutions available to detect attacks. Some focus on monitoring users and finding strange behavior. Others look closely at common attack targets such as admin accounts. The key is deciding which products will help you protect what is most important for your business.

Inspiring analytics

Yet risk mitigation isn't as productizable as cybersecurity. Compliance requirements vary by industry and local regulations. Fraud—a nearly universal problem for businesses—can be reduced using machine learning and analytics for detection and prevention.

Some of the biggest risks are operational or product-related and can have major impacts to a firm and its reputation. Not only are compromises in these arenas costly, but they jeopardize the trust of customers, impacting brand perception. Think of what occurred in 2016: Wells Fargo's problems with opening unauthorized accounts was an operational problem impacted the brand, reputation, and its bottom line. The Galaxy Note 7 fire issues (continuing with the S7) illustrates how a product risk can cascade to undermine an entire company.

Using the process outlined above of defining normal, monitoring against it, and protecting the crown jewels, you can use advanced analytics to better understand the particular risks your business faces. By also creating a risk-aware culture, employees can feed the system with early warning signs. This results in a positive feedback loop, in which data and analytics define normal and track out of the ordinary events, allowing you to identify and mitigate major risks before they cause lasting damage.

The great thing about taking a portfolio approach is that it enables creation of a risk identification and management system that is tailored to your business and its individualized needs.

This paper was created by CITO Research and sponsored by Teradata

CITO RESEARCH TERADATA.

Charles Griffith

Practice Director; Security and Fraud, Teradata Corporation

Business Consulting, Teradata Certified Professional

Charles serves as Practice Director for Security and Fraud within the Business Consulting Group. Prior to joining Teradata, Charles and his team developed and managed a very large and highly acclaimed Data Warehouse program that was covered in reviews by Computer World, Info Week, American Banker and others. Charles has provided thought leadership as a presenter at international conferences such as the American Marketing Association, UC Berkeley Fisher Center for IT, FIMA, DAMA, and Teradata Partners.

Dan Woods

Chief Analyst and Founder, CITO Research

I do research to understand and explain how technology makes people more effective in achieving their goals. I write about data science, cloud computing, and IT management in articles, books, and on CITO Research, as well as in my column on Forbes.com.