Technology enables firms to capture and produce more, so regulators inherently expect more.

Steve Marsh, CEO, Smarsh
# CONTENTS 2:2013

### 04 Copy that
Regulators, companies and surveillance professionals try to get a handle on unstructured electronic communication data.

### 08 Power rangers
Regulators in Europe will have access to centralized surveillance data, providing a comprehensive view of Europe’s energy market.

### 10 Know thy enemy
Cyber security is a core business risk, and companies need to develop strategies for sorting through the barrage of attacks.

### 12 Combined risk
With an efficient governance, risk and compliance (GRC) solution, companies can save costs and create transparency.

---

**A level playing field for surveillance**

Over the last decade, a significant amount of equity trading volume has migrated to broker-dealer operated alternative trading systems (ATSs). These exchange-like OTC trading platforms, including dark pools, have different levels of transparency and are only accessible to their participants.

To ensure overall market integrity, it is critical to subject all trading venues, including regulated exchanges and dark pools, to the same rigorous transparency and market surveillance standards.

The U.S. market is among the most fragmented in the world, and is setting an example for other markets that are opening their doors to competition.

Dark pools in the U.S. report their transactions through one of several Trade Reporting Facilities (TRFs). While dark pools do not have a traditional order book per se, they do provide certain data to an audit trail called the Order Audit Trail System (OATS) that is available to the Financial Industry Regulatory Authority (FINRA). FINRA aggregates data from exchanges and dark pools and integrates it into its surveillance patterns. However, because ATSs are not obligated to provide FINRA with full information on their order book activity, FINRA does not receive as much data from dark pools and other ATSs as it gets from exchanges. As a result, there are opportunities to enhance FINRA’s surveillance of these market centers.

There are also differences in operational transparency between dark pools and exchanges. Exchanges must file their operating rules with the SEC, but dark pools only have to provide a description of their order handling process, their customer base and their subscriber requirements. While exchange rules are publicly available and subject to notice and public comment, dark pools submit this more limited information confidentially to the SEC.

FINRA is reviewing how to better identify dark pool trading data and whether users are provided with adequate descriptions of how dark pools work. Participants’ activities are also monitored for misconduct. For example, regulators are reviewing whether trading in one venue is used to impact activity at another. These are important steps to ensure market integrity.

While we are making great strides in consolidating the information needed to conduct cross-market surveillance and to level the playing field for all venues, we are not there yet. Some outstanding issues will be addressed by new regulations and processes such as the Consolidated Audit Trail (CAT) and the recently adopted Market Access Rule. If approved, the SEC’s proposed Regulation System Compliance and Integrity (SCI) will replace voluntary compliance with enforceable rules on development, testing, monitoring and reporting of critical trading and systems technology issues. It is important that Reg SCI rules extend to all trading venues.

Most regulators agree that the quality of surveillance cannot vary by venue. Transparency and complete information aggregated across markets is the best remedy to protect investors.
Bermuda Stock Exchange launches X-stream Trading

Bermuda Stock Exchange (BSX) has launched X-stream Trading, providing BSX with world-class trading technology. The solution will strengthen BSX’s dedication to the development of Bermuda’s domestic market, fueling capital to the country’s small and medium businesses as well as BSX’s leadership position in insurance-related trading activity. BSX and its members will benefit from significant enhancements in performance, latency and throughput capacity by upgrading to NASDAQ OMX’s proven exchange technology.

NASDAQ OMX and Smarsh establish partnership

Smarsh®, the leading provider of hosted archiving and compliance solutions for email and electronic communications, announced a partnership with NASDAQ OMX to offer Smarsh archiving and compliance solutions to corporations, broker dealers, exchanges and regulators alongside NASDAQ OMX SMARTS market surveillance and compliance solutions. The combined solution will provide users with the ability to extrapolate additional value through the correlation of trading data with employee and customer communications, such as email, instant messages, mobile messages and social media posts.

NASDAQ OMX to offer pre-trade risk management to Nordic derivatives members

NASDAQ OMX has launched a new Pre-Trade Risk Management (PRM) service, Genium INET PRM, to its Nordic derivatives customers. Genium INET PRM facilitates real-time pre-trade protection to mitigate erroneous orders and transactions. Through the service, member firms that trade derivatives on the NASDAQ OMX Genium INET platform are able to monitor their own order flow, including their Sponsored Access and Direct Market Access (DMA) clients. The service also allows for general clearing members to monitor client transactions.

NASDAQ OMX and Smarsh successfully delivered to FCA

NASDAQ OMX and the Financial Conduct Authority (FCA), a newly established independent body that regulates the financial services industry in the U.K., announced that the FCA has officially gone live with NASDAQ OMX’s SMARTS Integrity market surveillance platform. The solution will enhance its monitoring of transaction reports across the U.K.’s financial markets. The FCA is leveraging the scalable and extensible NASDAQ OMX platform to enhance its coverage of current and future European legislation, such as the Markets in Financial Instruments Regulation (MiFIR) and Market Abuse Regulation (MAR).

SMARTS Integrity goes live across all markets at BM&FBovespa

BM&FBovespa and BM&FBovespa Market Supervision (BSM) have announced the official go live of SMARTS Integrity across Brazil’s equities, commodities and futures markets. BM&FBovespa’s Equities market has been working with SMARTS since 2011, and now Commodities and Futures will be monitored on the PUMA Trading System platform. “Since Brazilian trading activity has grown in importance in the portfolio strategies of investors worldwide, it is crucial to provide local and international players with market surveillance tools that are aligned with the fully transparent and centralized order driven price discovery across all products in our marketplace,” said Cicero Vieira, Chief Operating Officer of BM&FBovespa.

OTC clearing and risk management live on KDPW_CCP’s OTC post-trade platform

NASDAQ OMX announced that its OTC clearing and risk management solution, Sentinel, is now live on KDPW_CCP’s post-trade platform. The NASDAQ OMX technology supports the Polish clearing house and CCP’s (central counterparty) trade lifecycle and risk management requirements for clearing of OTC traded instruments. “KDPW_CCP is utilizing NASDAQ OMX’s Sentinel technology as part of its KDPW_OTC clearing system to provide the robust real-time risk management required by our clearing members,” said Iwona Sroka, President and CEO of KDPW_CCP. “We aim to maintain our leadership role as Poland’s de facto clearing house.”
INANCIAL FIRMS in most countries are subject to data archival, retrieval and retention requirements. They must retain copies of unstructured electronic communications including emails, instant messages, social media, audio (i.e. voice mail) and video files. Ultimately, linking this communications content to trade surveillance results can provide new insights into a firm’s trading activities.

Capturing and analyzing unstructured electronic communications is critical. The types of communications are increasing, and volumes are growing exponentially. In addition, data must be stored in a format that cannot be altered. In the U.S., for example, data must be stored on tamper-proof media known as write once read many (WORM) in at least two places.

Analyzing unstructured electronic communications data can be particularly challenging. Electronic communications monitoring programs vary depending upon best practices for the type of financial institution and jurisdiction. Generally, compliance personnel and regulators look for an array of possible violations to established policies: pre-dissemination of material non-public information, insider trading, market abuse and manipulation, prohibited and inaccurate commentary, and inadvertent and inappropriate information leaks. They may check for misrepresentation or omission of important information pertaining to securities, fraud and theft of customer funds, violations of broker-dealer responsibilities and investor complaints.

OFTEN IT TAKES TIME for regulations to catch up with technology advances and changes in behavior. Capturing and analyzing unstructured data in electronic communications is no exception. Existing laws were drafted to cover traditional written communications and...
are difficult to apply to real-time social media, where people are constantly connecting, often across multiple geographies.

“Financial services is a relationship business. People develop tight relationships with certain customers and then connect with them on their personal Facebook or LinkedIn accounts,” says Frank Eliason, Director, Global Social Media, Citi. “That’s happening whether a company wants to embrace it or not.”

FINANCIAL SERVICES firms face significant risk associated with business communications via social media. For starters, social media is often used to distribute malware, which exposes firms to unauthorized access, misuse of information, phishing and spoofing.

Further, broker-dealers may be held accountable for staff online activity even when the company has no knowledge of their behavior. Employees may be communicating in an insecure manner, i.e. private messages sent on Facebook do not reside on the firm’s servers, so the firm does not control that information.

Eliason believes it is crucial to educate employees and customers about what can and cannot be communicated this way and explain the social media policy to all employees during standard compliance training.

“We have a policy preventing anyone from taking pictures inside our buildings, and we need to explain to employees why we have that policy,” he says. “One reason is we don’t want them to accidentally capture an image of a computer showing customer data on the screen. Distributing a picture like that on social media could have serious consequences.”

FIRMS THAT OPERATE in multiple jurisdictions face conflicting regulatory and legal challenges. In certain instances, they may not have the legal right to capture information in one jurisdiction, but it may be mandatory in another. To illustrate, in the U.S., the SEC and FINRA require firms to monitor social media they use for business purposes. FINRA’s Regulatory Notice 10-06 gives guidance to members on their use and risk management of social media. Meanwhile, more than 30 states have either passed or proposed legislation prohibiting companies from requiring access to employees’ Facebook accounts as a condition of employment.

“As a matter of practice, financial institutions can access that information, and SEC rules trump state statutes,” notes Steve Marsh, CEO of Smarsh, which provides hosted solutions for archiving electronic communications.

YEARS AGO, encryption responsibilities made it difficult for U.S. broker-dealers to carry out their surveillance responsibilities. For example, certain states required encryption of all communications that contained sensitive investor information, which meant that copies of archived emails typically could not be searched or analyzed.

“Over time these conflicts are resolved, but in the short term it becomes a question of who you want to appease most,” Marsh adds. “Typically firms that operate in multiple jurisdictions, or that have to satisfy more than one regulator in the same country, develop a strategy for resolving conflicts before they get to court.”

EU data protection rules, including Directive 95/46/EC which regulates the collection, processing, sharing and storage of consumer data, are a case in point. The SEC may require U.S. firms to capture communications pertaining to their overseas business, but the EU may prevent certain communications from being sent to the U.S. for storage. However, there are safe harbor procedures firms can follow to make that achievable.

Since the laws and regulations governing electronic communications are not uniform across the globe, it is important for business managers to partner with their firm’s legal department and with regulators to solve conflicts.

“The world is a smaller place on both a personal and business level, and people don’t necessarily think of borders the way they used to,” says Citi’s Eliason. “For us, it’s not Citi India or Citi Singapore; it’s one Citi. It’s becoming a question of who you want to appease most.”

REGULATORS MAY REQUEST data to support trades and check for various compliance violations.

Firms may also be asked to prove that they retain their electronic communications and can produce them quickly. For example, they may have to produce all messages involving a group of individuals that mention a specific topic or security within a given time frame. Besides these routine tests, regulators may make more targeted requests related to particular investigations.

**HASH CRASH**

On April 23, 2013 a hacker sent a false tweet, apparently from the Associated Press, reporting an explosion at the White House injuring President Obama. The stock market plunged 143 points immediately and rebounded once market participants learned the tweet was a hoax. The so-called Hash Crash did relatively little damage. However, some fear that if it fortified the negative perceptions of the market structure developed following the 2010 Flash Crash. The incident has implications for market surveillance professionals. As of this writing, the perpetrator has not been caught, so the motive for the prank is still unknown. Yet such a tactic could potentially be used to manipulate financial markets. It also proves just how fast word travels in social media, so it is critical to listen carefully to what is being said on the key platforms.
“The requests have gotten more complicated, and regulators are asking for larger data sets as they’ve gotten more advanced in their technology use,” Marsh observes. “Technology enables firms to capture and produce more, so regulators inherently expect more. A complicated query may involve 100 individuals talking about 50 securities over a certain date range along with certain types of attachments or links to third party web sites.”

Firms must be prepared to provide all data and information requested by regulators in a timely manner. They need to show they have risk management policies and procedures in place for electronic communications and their social media program. Further, they must prove they have implemented a stringent code of ethics around trading, electronic communications and social activities.

Those that cannot pass muster run the risk of being penalized with litigation, damaging their reputation and incurring substantial fines. Recently, one U.S. firm was fined about US$9 million for email recordkeeping failures.

Bill Nosal, Associate Vice President at NASDAQ OMX, SMARTS Broker, points out that various types of monitoring and surveillance are typically conducted by both buy and sell side firms. “Surveillance traditionally has been conducted in silos with trade surveillance being assessed independently of communications monitoring. But it is prudent for firms to link traditional trade surveillance tools that leverage highly structured trade and market data with tools that store and analyze unstructured electronic communications data and extract related events.”

While best practices in trade surveillance and electronic communications monitoring exist separately, technology-driven approaches that link the two areas to meet new regulatory requirements for trade reconstruction and advancing behavior detection are only beginning to emerge.

“Financial firms should consider investing in enhancing surveillance capabilities for electronic communications and trading, which is considered key for a compliance function,” says Samantha Regan, North America Capability Lead for Regulation and Compliance at Accenture. “We recommend firms start to think about the integration or triangulation of the two sets of data to help them build a more comprehensive picture.”

New software can perform analytics, establish preventative controls and enable firms to leverage huge volumes of information to identify malpractice and compliance events. NASDAQ OMX’s Nosal and Accenture’s Regan agree that a penultimate solution should monitor, store and retrieve data and all relevant communications from both internal and external sources and match them appropriately to related order, trade and settlement activity. Such solutions should also provide robust enterprise content management capabilities, management dashboards and reporting capabilities, as well as the ability to run tests and monitor activities.

“It is important to show that the right data and information is being captured, and the right events within it can be identified,” says Nosal.

Financial firms typically have in-house capabilities to store data and manage technology, but they do not always have the expertise to construct...
queries, produce information and eliminate attorney-client privileged information. A service provider that captures content from many sources can assist financial firms with data production requests. However, providers must follow the firm’s stringent rules and allow it to access all data and information.

“The single most important thing that I would recommend is to test your system to make sure that you can produce information,” says Marsh. “Firms don’t struggle with information capture, but they get so overloaded that when it comes time to search for communications, they fall on their knees.”

TECHNOLOGY CAN BE deployed to scan electronic content for certain keywords, phrases, activities or behaviors that may suggest suspicious activity. Some solutions leverage integrated data and analysis tools to allow an investigator to cross data sets and examine activity. They can also examine the relationships and interactions between employees and with trade counterparts. They model an employee’s networks across platforms and look for deviations from the norm.

There are proxy-based tools that allow employees to access their presence on social media platforms from the company’s internal network, and the company can monitor employee activity. Firms can build rules so some activities are permitted automatically while others require approval. For example, the tools might automatically flag a communication from an investment analyst who puts a buy or sell recommendation on Facebook, or they may prevent that person from going on Facebook altogether.

Yet some employees may be cautious about this method of social media access. For example, LinkedIn is used for recruiting purposes, and employees do not want their current employer to track these conversations.

“If they are not comfortable with that access method, either they won’t use it, or they’ll bypass it entirely,” Elia-son warns.

With proxy-based tools, users think they are connected directly to a particular social media platform, but they are not. They are effectively passing through a filter which monitors their activity, preventing unauthorized access. However, these methodologies generally work only within the firm’s network or from company-managed devices. Firms can still be held liable for employee wrongdoing while communicating elsewhere. As a result, some firms prefer to use a hybrid of proxy-based tools and connecting directly to the APIs of Twitter, Facebook and LinkedIn.

Yet Regan is cautious about key word surveillance because it may produce too many false positives. She advocates strengthening the data, closing potential compliance breaches and using thematic surveillance (constructing monitoring programs across different themes to accomplish better structure in surveillance work).

THE EXPERTS HAVE some parting advice for firms grappling with monitoring electronic communications and complying with regulations.

Data should be stored in its native file format; specifically, social media posts should not be converted to emails. Emails are flat and linear, and there is a communications thread. Social media posts are relational, and they tend to have objects such as pictures and documents that people comment on, like or forward. All those interactions need to be captured as they are.

“You can’t just take a snapshot of a social media page, convert it to an email and throw it into an email archive,” warns Marsh. “If you do that, you’re effectively altering the communication, which puts you at risk of tampering with it.”

Firms should ensure their electronic communications policy includes the use of mobile devices that are capable of email, instant messaging and text. Countries such as the U.K. require firms to capture cell phone conversations involving client trades.

Finally, by reaching out to companies in other industries — especially highly regulated ones such as pharmaceuticals — financial firms can share experiences, get new ideas and improve the effectiveness of their monitoring programs.
Europe’s power markets prepare to comply with new market surveillance mandates.

**Europe’s power markets** developed separately over time, each with its own nuances, rules and regulatory oversight. From a surveillance perspective, exchanges and brokers monitored their own trades, and national regulators watched over their home markets. Power companies monitored their own activity for compliance with market rules.

Several factors are driving change in this structure. First, the European Union has developed a road map for common standards as part of its single market strategy. Second, since the financial crisis, all market instruments and mechanisms have come under scrutiny, driven by the perception of excessive risk taking and the potential for systemic risk. In addition, the authorities have been working to align energy and financial markets regulation because derivative instruments are common to both, and there have been several high profile cases of alleged power market manipulation and anti-competitive behavior.

Against this backdrop, the REMIT legislation on wholesale energy market integrity and transparency was passed in December 2011 to prohibit market manipulation and insider trading in EU wholesale energy markets. The Agency for the Cooperation of Energy Regulators (ACER) is tasked with pan-European power market monitoring and collecting data from market participants. ACER recently selected the SMARTS Integrity market surveillance system to help it fulfill this role.

“Previously, incidents of manipulation were hard to detect because no one had systematic, timely access to all the data,” says Lorne Chambers, Global Head of Sales, SMARTS Market Surveillance at NASDAQ OMX. “Going forward, the regulators will have more data available to them much sooner after transactions are executed. Further, the data will be centralized, providing the relevant authorities with a comprehensive view of the entire market.”

ACER will receive data on every transaction, each with multiple data fields, so dealing with the quantity of data inputs will be a challenge. ACER will also need to drill down to understand what is going on behind the trades. For example, many large power companies operate multiple business streams; all could make commercial decisions separately, but trades could come to market through a single avenue. A company may sell at one price and moments later buy the same instrument higher – a behavior that might look suspicious but in reality may be fully justified.

Power companies will have to consider how much additional data they will need to store to build audit trails. Moreover, they will need to store information about internal pricing between desks. The banks already do this, but it is a new paradigm for many utilities and smaller municipalities. ACER will also need to monitor for unusual trading ahead of unexpected announcements, such as power plant shut downs, that can affect trading activity.

Once REMIT is implemented, all players will report data to a common platform. Standards of oversight, points of contact and information flow will be the same, but local market nuances will continue. The price of power is determined by the power producing options in each region along with any market coupling across borders. Since approaches vary, it is important to understand sudden price movements.

“We’re taking technology that has worked well in the capital markets and applying it to address similar challenges in the energy markets,” says Chambers. “At the same time, we need to figure out where some of the usual approaches might not work, considering energy market dynamics and come up with innovative techniques specific to energy markets.”

For now, power market participants are focusing on meeting their trade data reporting obligations under both European Market Infrastructure Reform (EMIR) and REMIT.

“They’re facing a big challenge because the requirements are not that clear yet,” says Aviv Handler, Founder and CEO of ETR Advisory.
and CEO of ETR Advisory in the U.K. “They have to plan their infrastructure to grab all the data they can for REMIT, while taking into account that requirements might change.”

ACER intends to source pre-trade data from execution venues, but it is unclear how that will be done. It is also uncertain whether market participants will be responsible for providing data to ACER if the execution venues cannot provide it. At this stage, market participants are working out where they will get the trade data they need to report to the authorities and whether to report it directly to the repositories or to use a reporting service.

Most banks and some of the larger utilities already maintain internal market surveillance systems. While it makes sense for mid-sized and smaller companies to implement similar platforms, that is a secondary priority. It is still unclear if internal surveillance will be required under REMIT.

“If I were a trader, I would want to know if my firm is suspected of market manipulation before the regulator and the press find out,” says Handler. “That way if it’s leaked, I can tell the market I’ve already resolved the situation. A lot of companies aren’t preparing for that.”

Electricity and gas bills are rising, so the public is very interested in how the price of power is set. The regulators need to ensure that market participants are not engaging in abusive practices that could impact consumer pricing. REMIT will go a long way toward achieving that goal.

The implementation dates are constantly moving, and there is a danger that market participants will start relying on delays as part of their strategy. Until ACER starts conducting investigations, no one knows what questions will arise. But one thing is certain: armed with a centralized surveillance system, ACER will be equipped to ask the right questions.

ACER’s surveillance obligations
Going forward, each country’s National Regulatory Authority will oversee physical electricity trading, and the Competent Authority will be responsible for derivatives trading. ACER will monitor all electricity and gas markets for abuse, identify potential cases and conduct preliminary investigations. Enforcement responsibility will lie with the relevant regulator or will be shared for incidents involving both derivatives and physical markets.

The European Commission’s “Implementing Acts” will provide the technical standards for market participants to comply with their obligations under REMIT. The Acts will mandate the data that must be reported to ACER and in what format.

The target date for the Implementing Acts to come into force is in late 2013.
STAYING ONE STEP AHEAD

The financial industry must develop a strategy for thwarting advanced persistent cyber threats.

Illustration: Jesse Lefkowitz

CYBER SECURITY THREATS from criminal organizations and industrial espionage have long plagued the financial industry. In another concerning development, some ideologically based cyber actors have been trying to disrupt business operations and, in certain cases, destroy data. As these adversaries have gotten more technology savvy and global, they have become bolder and more disruptive. The Internet makes spying much easier because no foreign travel or physical access is necessary. Moreover, it is difficult for companies to detect when they become victims.

Discussions about cyber security often focus on harvesting intellectual property (IP). Like other companies, exchanges and broker-dealers tend to take false comfort in the fact that their IP (often their source code) is protected. But adversaries have gone beyond that. Their core mission is often industrial espionage.

“Adversaries have figured out that they can be successful in their own businesses by mirroring a company’s tradecraft and technology,” says John Watters, CEO and Chairman of iSIGHT Partners, a global cyber intelligence firm. “They want to understand its entire business methodology – its mechanisms, pricing models, supply chain, customers, strategy and tactics, so they can replicate the business models with lower labor costs.”

ONE WAY AN ADVANCED persistent cyber threat may be launched is through proactive “spear phishing.” An adversary will email a significant percentage of a company’s employees asking them to click on a link to a web site laden with malware. A “watering hole attack” is when the adversary identifies a site that targeted employees may be particularly interested in and then infects that site with malware.

Typically, there are multiple stages of infection on the network, compromising many systems. The attack is persistent because the software can remain undetected for a long time. Once a system is compromised, the intruder can issue commands that cause hidden programs to disrupt operations enterprise-wide.

“Adversaries will face each other with the ability to produce ‘mutually assured downtime (MAD),” says Mark Graff, Chief Information Security Officer at NASDAQ OMX. “This could be a significant problem for exchanges and broker-dealers; they are constant targets and are always concerned about ensuring system uptime and availability.”

There are billions of cyber security events daily. The sheer volume makes it impossible for companies to focus on every threat.

“Adversaries intentionally create noise – discrete events that gener-
ate security alerts – to keep you from finding actual signals related to real attacks,” Watters explains. “The key to preventing attacks is how you find the signals in the noise in your environment.”

Toward that end, iSIGHT Partners’ methodology involves building playbooks of attack methods and their associated threat indicators (i.e. MD5/Hash/IP/URL). Security technologies can generate alerts and connect these threat indicators back to the context, adversary and objective. Incident indicators (alerts from the security technologies) are mapped to the threat indicators derived from the threat environment. As a result, organizations can prioritize security resources, focus on high impact threats (signals), and allow security technologies to deal with low impact threats (noise).

“The only way companies can deal with the traffic volume in their security systems is to shrink the size of the problem and limit the number of addressable threats to a manageable number,” Watters maintains. “Even in large organizations, the number of security events that most organizations can deal with is less than 10 per day. Selecting the right 10 events to focus your efforts on will define your security team as effective and efficient cyber risk managers.”

Exchanges and broker-dealers need to control what comes in and out of their networks and ensure that what is on the network is supposed to be there. To do so, they establish multiple filters, ranging from traditional firewalls to more sophisticated techniques that search for malware. Firms also block intruders by checking software against sites known to be rigged with infected software. Further, employees can be required to log on to the Internet using a user name and password.

Security staff typically scan all machines for viruses and infections and monitor traffic flow between machines to prevent one machine from infecting another. But they also need to pay special attention to parts of the network that may not be considered important to everyday business.

“Backwater systems, such as unused servers that are still in operation and workstations that are connected some of the time but aren’t upgraded with antivirus software potentially provide a space for attackers to hide out,” warns Graff.

**TO PREVENT PROACTIVE** spear phishing the security staff can teach employees how to spot suspicious emails. A typical activity is to occasionally send employees questionable emails and provide additional training for those employees who click on the links.

Many financial market participants will automatically advise law enforcement of successful attacks. Getting the intruders out and keeping them out, however, requires skilled staff trained to look for anomalies in the displays and logs of the various intrusion detection devices. At the same time, a strong firewall is critical to keeping them out in the first place.

Companies typically spend 3-7% of their IT budget on security, while highly targeted firms spend up to 5-10%. Graff and Watters agree that many organizations today under-invest in threat intelligence, viewing cyber security as primarily a technology and compliance issue. Yet cyber security is a core business risk that affects corporate strategy and how companies conduct business and must be managed accordingly.

The best approach to managing risk is to assess potential threat scenarios, understand the attack methods associated with these threat scenarios and build a focused security organization that looks for, detects and defeats high impact threats.

“If you build your security organization that way, your security technologies will handle the noise, and your organization will be focused on the signals,” says Watters. “That’s how you manage the most risk per dollar invested.”

---

**TAKING PREVENTATIVE ACTION**

- Establish policies and procedures ahead of time so you are not improvising should an attack occur.
- Gather intelligence so you can identify high impact alerts and prioritize which to tackle first based on recognized business needs.
- Have equipment in place, so you can check your firewall and the logs that are created by various intrusion detection devices and look for anomalies.
- Identify your major concerns (confidentiality, availability, integrity), and build these factors into your policy for protecting core systems.
- Periodically conduct proactive scans and have experts evaluate your systems.
A holistic view of risk

An integrated governance, risk management and compliance (GRC) solution empowers exchanges and broker-dealers to track, measure and manage risk across the enterprise.

Traditionally, broker-dealers and exchanges have managed risk in silos, and as a result, they often duplicate efforts across the enterprise. More importantly, they may miss out on adequately managing certain risks. With increasing regulations and greater exposure to financial and reputational risks, firms are turning to Governance, Risk Management and Compliance (GRC) solutions to provide a holistic view of their total risk exposure and to manage it more effectively. Ultimately, this enhances their ability to execute their strategy, to create shareholder value and to comply with regulations ranging from Basel III to Dodd-Frank and Sarbanes-Oxley.

Brazilian exchange streamlines GRC

BM&FBOVESPA, the third largest exchange in the world in terms of market value, is using BWise, a NASDAQ OMX company and a leading GRC solutions provider, to support its internal audit and enterprise risk management processes.

“Once implemented, the system will measure risk in corporate and business processes, and provide controls for risk mitigation,” says Gustavo Baptista de Araujo, Audit Officer at BM&F Bovespa. “BM&FBOVESPA will be able to closely monitor risks in real-time and over time, identify control gaps as well as ineffective controls.”

Understanding the spectrum of risks is the foundation of GRC. Among the key risks for exchanges and broker-dealers are information security, data theft, terrorism, business continuity and market abuse. These potential threats could have a significant impact on an organization’s strategy and operations. In addition, regulators can impose steep fines to firms that do not measure, monitor and manage risk properly, and the firms can suffer reputational and financial damage that, in severe cases, can lead to their destruction.

Without an integrated system exchanges and broker-dealers duplicate their GRC efforts. According to Luc Brandts, CTO of BWise, a NASDAQ OMX company, these organizations spend as much as 5-10% of their annual budget on risk and compliance. Not only is this an enormous amount of money and a huge burden, but funds spent purely on compliance are not spent on revenue generation.

He advises firms to tackle GRC using both a top-down and bottom-up approach. A top-down approach involves defining the strategic and operational risks that must be managed. That may vary depending on the structure of the business and the geographies in which it operates.

“In Southeast Asia, for instance, business continuity is top of mind because floods and other natural disasters are relatively common,” he points out. “Similarly, Hurricane Sandy opened up a whole different set of discussions in the U.S.”

A bottom-up approach involves making sense out of the data in the firm’s systems as well as the risk alerts they generate. With a GRC system, users can address individual cases alert by alert, compile a strong audit trail for each and identify new risk controls that may be required in a comprehensive way.

By integrating processes, internal controls, compliance and internal audit, exchanges and broker-dealers can simplify their risk management structure as well as ensure rigorous governance and an effective control environment. They can provide a holistic view of their risk to the board and audit committee, who in turn can provide feedback on their risk appetite. Finally, they can establish and manage action plans and promote a corporate culture where risk assessment is incorporated into all levels of decision-making.