Look deeper into data to spot security threats
Leveraging analytics to find patterns and vulnerabilities
Modern businesses rely on their data – on the ability to mould data into useful information they can use to identify opportunities, to serve and retain customers, and to communicate with partners. Criminals rely on that data, too. They rely on it to identify security holes, to steal from companies and consumers, and to maim critical networks.

Smart organisations know the steps they must take to fortify their data – their information and networks – to repel and deter cyber criminals. Smarter organisations know that cyber criminals continue to find ways around those fortifications. Smarter organisations also know the importance of emerging technologies to spot the criminals before they can do any real damage. Increasingly, analytics tools and techniques are offering solutions for organisations who want to do more than repel cyber invaders.
Seeking opportunities

Cyber criminals aren’t easily deterred. Their job is to find security holes, not to run away when they run into security obstacles. When they don’t get in and do damage, you don’t know about the attempt. But you need to know it. Just as criminals look for opportunities to worm their way into your organisation’s data and networks, your organisation needs to look for opportunities to spot activities that indicate an attempted intrusion.

The intrusion threat evolves as hacker technologies, hackers’ know-how and technologies you use to do business, evolve as well. The picture is always changing, and your organisation needs a plan for how to view and interpret that picture. Your organisation needs a cyberanalytics strategy.
A continuum of considerations

Key questions

Cyber attackers continue to up their game, and as organisations attempt to get ahead of attackers, deploying cyberanalytics strategically becomes paramount.

Thinking about where you stand now is important. But thinking about where you’re headed is also critical. Pondering some essential questions on data and analytics can help you get in the right mindset to move forward with cyberanalytics solutions that can address evolving threats and your organisation’s evolving needs.

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where does your data reside and how easy is it for you to “see” that data now?</td>
<td>Hackers can spend all day trying to find out where your information lives. If you don’t know where all your data resides and how to access it, you may already be playing a game of catch-up.</td>
</tr>
<tr>
<td>What analytical tools do you have in place, and how well do they work?</td>
<td>The tools you have today might not be enough to address all the challenges of tomorrow. But it’s important to know the effectiveness of the tools you use now to make decisions about new needs for analytics tools and prioritise deployment of cyberanalytics solutions.</td>
</tr>
<tr>
<td>What additional types of data will your organisation need to do business in the year ahead?</td>
<td>Business needs shape the types of data that your operational units will collect and leverage. Hackers will plan on you acquiring new data – viewing new sources of data as new points of attack. Your cyberanalytics strategy needs to take into consideration not just the types of data you have now, but the types of data your organisation will be producing or developing in the months ahead.</td>
</tr>
<tr>
<td>What future organisational activities may require you to manage or analyse more data?</td>
<td>New directions, new markets, and new activities portend the potential to create data. Think ahead of the data and the activities that spawn the data. Become aware of the business direction of your organisation so you can put in place cyberanalytics solutions in a timely manner – analysing data for cyber threats the moment new offerings, new markets, or new partners go live.</td>
</tr>
</tbody>
</table>
Seeking the right solution

Knowing the key questions and having some good answers will take you far toward developing a cyberanalytics strategy. Ultimately, you’ll want a “true” cyberanalytics solution. As you seek the solution or solutions that will work best for your organisation, awareness will be essential.

Be aware of solutions that aren’t what they appear to be. Many vendors will label their technology solutions as “analytics” even though they fall short of being true analytics solutions. For example, a vendor might call a network-forensics tool an “analytics solution”, even though the tool lacks the predictive and pattern-spotting functionality that defines a “true” solution. Analytics involves detecting patterns and outliers, and a true analytics solution should address that need while allowing an organisation to move through the “lifecycle” of data analytics – from real-time to long-term.

Keep a phased approach in mind. No matter where you start with cyberanalytics, be prepared to extend your strategy and your cyberanalytics solution to other areas. And know that you ultimately will need a combination of technology products across all three phases of the cyberanalytics continuum. One solid approach for many organisations is to start with a real-time analytics capability and then build toward mid-term and long-term analytics capabilities.

Understand the enabling technologies at play. Cloud, mobile, and social technologies all present unique challenges and considerations in the realm of cyberanalytics. As others host your data in the cloud and as you seek to analyse it, you could face issues with data latency or lag. While real-time analysis can work well in the cloud, long-term analysis proves more challenging.

When it comes to mobile technologies, your organisation may not see much need for cyberanalytics since malware threats have not bloomed into a major challenge in the mobile realm. But more mobile threats are on the way. Have an analytics strategy to deal with them.

And with social media, understand that activities on the social front can offer clues to the cyber threats that are coming your way. Political, economic, and social protests can spill over from the social media realm and manifest as cyberattacks on high-profile targets. Your organisation could end up in the crosshairs.

Understand the threats and the role of cyberanalytics in your industry. All organisations tend to share some common themes when it comes to cyber threats and analytics. The threat of malicious insider activity and the misuse of data-access privileges can touch any organisation. But there are unique considerations for various industries, and different challenges will require different cyberanalytics strategies and tools.

Financial services and insurance companies tend to face “omnichannel” fraud threats. For example, attacks come not just in cyber form. They come via customer-service phone calls in which an attacker may attempt to access a consumer’s data without authorisation. They come via attempts at phony transactions at the teller window. And they come as more routine online attempts to access protected data.

In the health sector, detecting misuse of personally identifiable information represents a central cyberanalytics concern. And in the energy/resources sector, organisations need to remain mindful of the potential for theft of service, vulnerabilities with smart-meter functions and data, and abusive access of data. Energy/resources organisations, as part of the nation’s critical infrastructure, also continue to represent targets for conventional cyberattacks.

Identifying your next step

Staying ahead of cyber threats takes work, and the work begins with knowledge. A true cyberanalytics solution can serve as a valuable resource to let your organisation gain knowledge by identifying and predicting cyberattacks - or even conventional fraud attempts. Improved cyberanalytics offers a knowledge solution, and Deloitte can provide assistance in building that solution. We have extensive experience in the realms of data, analytics, and security. We can also offer help addressing a range of needs, from strategy and policy development to solution selection and implementation.
Contacts

Navin Sing
Managing Director: Risk Advisory Africa
Mobile: +27 83 304 4225
Email: navinsing@deloitte.co.za

Derek Schraader
Risk Advisory Africa Leader: Cyber Risk Services
Mobile: +27 82 330 7711
Email: dschraader@deloitte.co.za

Werner Swanepoel
Risk Advisory Africa Leader: Data Analytics
Mobile: +27 82 442 5948
Email: wswanepoel@deloitte.co.za

Cathy Gibson
Director: Risk Advisory Southern Africa
Mobile: +27 79 499 9046
Email: cgbison@deloitte.co.za

Henry Peens
Associate Director: Risk Advisory Southern Africa
Mobile: +27 82 496 8694
Email: hpeens@deloitte.co.za

Tricha Simon
Risk Advisory Regional Leader: Central Africa
Mobile: +263 772 234 932
Email: tricsimon@deloitte.com

Julie Nyangaya
Risk Advisory Regional Leader: East Africa
Mobile: +254 720 111 888
Email: jnyangaya@deloitte.co.ke

Temitope Aladenusi
Director Risk Advisory: West Africa
Mobile: +234 190 41730
Email: taladenusi@deloitte.com
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (DTTL), its network of member firms and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries and territories, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte’s more than 225,000 professionals are committed to making an impact that matters.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms or their related entities (collectively, the “Deloitte Network”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2016. For information, contact Deloitte Touche Tohmatsu Limited

Designed and produced by Creative Services at Deloitte, Johannesburg (CIC/Vee)