Borderless Behavior Analytics

Who's Inside? What're They Doing?

Second Edition

Saryu Nayyar
CEO, Gurucul Solutions, LLC

Contributors:
Jerry Archer – CSO, Major Financial Services Company
Devin Bhatt – CISO U.S. Federal Agency
Nilesh Dherange – CTO, Gurucul
Gary Eppinger – CISO, Carnival Cruises
Gary Harbison – CISO, Monsanto
Leslie K. Lambert – CISO at Large
Jairo Orea – CISO, Kimberly-Clark
Robert Rodriguez – CEO, SINET
Jim Routh – CSO, Aetna
William Scandrett – CISO, Allina Health
Joe Sullivan – CSO at Large
Teri Takai – CIO at Large

Senior Contributing Editor – Patrick S. Barry

BORDERLESS BEHAVIOR ANALYTICS
Who's Inside? What're They Doing?
Second Edition

For more information contact:
Gurucul Solutions, LLC
www.gurucul.com

Publisher: Ankur Chadda
Managing Editor, Second Edition: Leslie K. Lambert
Managing Editor, First Edition: Tom Clare
Graphics: Raghunath Sontakke
Cover Design: 99 QUEEN

ISBN: 13: 978-1986763332

"There are only two kinds of companies.
Those that were hacked
and those that don't yet know they were hacked."

Popular Cyber Security Credo

"The world has changed.
Security and data will be something
that goes on for hundreds of years in the future.
We are at the beginning of that stage."

Tim Armstrong – CEO, AOL

.

BORDERLESS BEHAVIOR ANALYTICS

Who's Inside? What're They Doing?

Second Edition

CONTENTS

ACKNOWLEDGMENTS

Vishal Salvi, Renee Guttmann-Stark,
Craig Cooper, Tom Clare,
Ankur Chadda, Craig Kensek

Special Acknowledgment
from the Publisher and Managing Editor

We would like to recognize Patrick S. Barry's invaluable contribution to the development of both the first and second edition of this book. He has been the driving force for many aspects of this project and his marathon of dedication to excellence and this book is deeply appreciated.

Foreword

Digital transformation (DT) means different things to different people. Its purpose is all about providing ideal connectivity, where an organization's different systems are seamlessly integrated, delivering the most optimal user experience possible. To achieve this objective requires building the right ecosystem with numerous processes and process optimization. This all means greater opportunity, yet amplified challenges at the same time.

Looking at DT from an IT perspective, as a large IT service provider, my company, Infosys, has numerous digital transformation programs focused on the transition of legacy applications into what organizations need to modernize and facilitate the demands of a state-of-the-art ecosystem. These initiatives often employ new technologies empowered with strong machine learning, AI models, integrating with open source solutions, APIs and more. Yet there's another consideration that must be taken into account to ensure a successful digital transformation: It must all be safe and protected.

Concerns from a CISO's perspective relate to the perpetual challenge of delivering the assurance of data integrity and confidentiality to their stakeholders. This represents a significant conundrum due to the broad array of complex technologies involved. The popular analogy for security experts is that we're mid-flight on an aircraft, where we must fix all problems onboard, maybe even change the wings, while we're flying! To a traditional security practitioner it may seem an impossible task, yet to the forward-looking CISO, this is their new normal.

Amplifying that challenge, a number of the resources CISOs require have not yet been fully developed. As well, the role of CIO is rapidly changing. All the books they've read relating to controlling technology and infrastructure approach obsolescence. The old rules are going away. For our profession to successfully embrace the future challenges posed by DT, we must have more agile and adaptable cyber security programs. This means being able to make leapfrog changes, and not be shackled by methodologies of the past, where we otherwise remain two or three cycles behind in technology innovation.

The adaptable agility required today for emerging cyber security programs exists in the realm of borderless behavior analytics. This class of security analytics addresses an increasingly porous security perimeter challenged by the expanding use of IoT, mobility, BYOD and the onslaught of widespread cloud adoption. Except for unique circumstances and requirements, the standalone monolithic on-premises environment has become a footnote in tech history. On-premises environments, while they remain important for many organizations for the foreseeable future, represent a fractional and a continuously diminishing element of the larger DT landscape.

How do borderless behavior analytics contend with this extreme complexity?

Building solutions, systems and processes that ensure optimal data integrity and confidentiality for information stakeholders, plus providing holistic monitoring of behavior, are acknowledged as keys to success. With those capabilities, we can analyze behavior across all aspects of the work humans do; by adding entity activity, this further enables us to identify and predict good or bad behavior. This entails a comprehensive mapping of hybrid environments, the identities within them, and building algorithms that quickly and reliably identify any outliers, to deliver effective attribution of true positives for risk-based security alerts. As well, there's a need to continually improve these capabilities as criminal threat tactics evolve.

Driven by mature machine learning, and drawing context from big data across an environment's data silos, the power of user and entity analytics (UEBA) delivers the capability for that one hop to quick attribution, which in the past had been fundamentally impossible in a complex IT environment. To identify who that one person, that one identity, is associated with a particular malicious act is crucial. Because of that, I believe there's great promise for UEBA in the future. It all depends on how models mature and in turn reliably identify and predict the evolving range of bad behaviors with accuracy and rapid attribution.

Security leaders must make their own assessments to support the future planning required for a successful DT initiative, and decide on the three or four areas where they'll bet big as far as their long-term security strategy is concerned. In the past, SIEM (security information and event management) solutions were one of those big bets, which in the long term failed to continue delivering the enduring value many experts thought they would. When it comes to technology, the CISO's journey, it will always be an evolutionary one. From the advanced security analytics focus, this book, now in its second edition, represents one of the important new entries in the CIO and CISO's library, to assist in that journey, to realize the promise of digital transformation.

Vishal Salvi
CISO, Infosys

Vishal Salvi is Chief Information Security Officer and SVP at Infosys. Vishal has more than 24 years of industry experience in IT service delivery and cyber security with positions at Crompton Greaves, Development Credit Bank, Global Trust Bank, Standard Chartered Bank, HDFC Bank and PwC. He performed leadership roles in cyber security at these organizations for over 18 years, with his previous role serving as a partner in cybersecurity practice at PwC. Vishal has extensive management and domain experience in driving the information and cybersecurity programs in all key aspects A well-known leader in information security industry within India as well as globally, Vishal has rich experience delivering large scale, mission critical projects on time and under budget.

Introduction

With the advent of ubiquitous mobility and ever-expanding cloud adoption, humanity has crossed the threshold into a brave new world, yet not everyone knows that nor understands the implications. Yet the number people lacking that understanding has lessened somewhat through the benefit of the first edition of this book, with over five thousand copies in circulation among today's security community, and with demand still going strong. Indeed, the praise for the book has been gratifying. Once example is Dan Lohrmann, of the online magazine *Government Technology*, who gave a rave review for the first edition of the book, stating *"...this is a MUST READ for understanding the next generation of security solutions..."* Providing that kind of needed resource is why we're determined to provide the second edition of this book with expanded insights.

This passage into a new reality of security requirements simultaneously represents profoundly exciting possibilities, delivering empowered productivity and enhanced cost savings, and, at the same time, ushers in sobering trends in risk management. Those who understand this transition stand in position to take advantage of the possibilities, as well as to protect themselves against the perilous developments inherent in the journey. We have, in effect, left the comparatively safe confines of a modern suburban world and now find ourselves in something of a Wild West frontier, replete with the legendary gold rush where fortunes can be made overnight, or livelihoods may be destroyed by misguided actions based on uninformed perceptions and weak strategic decisions.

With the rapid and widespread adoption of mobile devices, along with the IoT (Internet of Things) becoming integrated into the most intimate niches of our lives – from bio wristbands that count our steps and monitor our heart rate, to applications on our mobile phones that budget our calorie intake, and keep us up-to-date with the inventory in our refrigerator – the massive amount of human data has ballooned to staggering proportions. Experts forecast this digital exhaust will reach 44 zettabytes by 2020. ABI Research estimates the global wireless connectivity market (excluding cellular), will exceed 10 billion integrated circuit (IC) shipments annually by 2021. This ocean of data, and data delivery nodes, is not only growing rapidly to gargantuan proportions, but the unique and complex segments in which data resides is expanding and evolving, as well. Now in business, the same rapid and widespread explosion of digital exhaust generated by both mobility and cloud adoption inside the enterprise has reached beyond the capabilities of human analysis. The security perimeter has been blurred and for most intents and purposes, simply faded away.

Organizations are seismically impacted by this paradigm shift of cloud and mobility as they strive to adjust to the manner in which their employees and customers use and manage technology. The infusion of bring your own device (BYOD), high-speed internet connectivity and the use of cloud-based applications are continually redefining enterprise networks, not through proactive planning and change management, but in an ad hoc reactive manner. The use profile is 24/7, global, instantaneous, and rich in consumer-driven IT. Everyone is accessing everything on the internet, all the time, and in a staggering volume of activity. At the same time, however, there persists a comparatively low awareness of the risks associated with access and activity, plus their importance, among the general population of today's employees. This reality courts disaster, enabling more emerging undefined gray areas of risk than declarative defenses can ever address. A new awareness of access and activity risks is urgently needed and one from a risk-based solution perspective which holistically quantifies risk as quickly as possible.

Gone are the days when attacks on a system such as internet worms, email spam and opportunistic hacks were the prevalent security issues of the day – which have been addressed through the layering of defense-in-depth technologies such as firewalls, antivirus software and spam filtering mechanisms. Intellectual property and regulated information no longer resides only behind firewalls; this singular control point of protection has disappeared. Instead, there's a much more complex hybrid IT security challenge of on-premises environments being connected to a host of cloud applications, all being accessed via an expanding array of mobile devices.

An enduring popular quote among security pundits is, "There are only two kinds of companies. Those that have been hacked and those that don't know they've been hacked." Now, however, attacks against any business are likely to be stealthier, targeted in a far more sophisticated manner, while always changing and evolving. Nation states and highly skilled individuals, with vast resources and seasoned knowledge of the most effective way to attack companies' vulnerabilities, carry them out. They move quietly within organizations, sometimes for years, rather than months, moving laterally throughout the computing environment, steadily acquiring everything they need for their malicious assaults.

At the root of modern threats is the compromise and misuse of identity which gives the attacker access to the keys of the kingdom. Identity is the critical access mechanism, a threat plane unacknowledged by far too many organizations. With identity-based access, attackers easily bypass declarative defenses based on static rules, signatures and patterns. Traditional defenses identify known bads (red) and safe profiles (green). Yet with identity as a primary risk, attention must now be focused on the vast gray areas between the red and the green. This is why a new form of risk management, which includes precise risk scoring, extracting context from big data, moving from detective to prescriptive, has become so essential.

With most traditional security solutions focused on prevention, and detection, the impact of these emerging influences on older security systems is profound. Firewall, security information and event management (SIEM), intrusion detection systems (IDS), intrusion protection systems (IPS), data loss prevention (DLP), vulnerability assessment, sandboxing – were all primarily designed to look for, to detect, the known, often from the outside. While this has been effective for preventing and detecting a specific class of external attacks, these techniques rarely expose the malicious insider because they're moving through the environment exploiting approved access. The majority of organizations' access privileges are far too over-provisioned. Industry experts observe that most Fortune 500 companies have 50% or more of their privileged access occurring outside sanctioned account lists and vaults as hidden unknowns. In one specific real-world use case, Gurucul's direct solution delivery experience observed a large enterprise where they discovered over 70% of their privileged access had been unknown, hence ineffectively controlled, or uncontrolled, including application privileges representing serious and unrecognized risks to the organization.

More concerning, insider attacks are on the rise. According to Verizon's *2017 Data Breach Investigations Report (DBIR)*, a 46% rise in insider threat occurred over the last year, where network intrusions have involved employee identity and weak credentials. In addition, existing traditional identity management solutions are not designed to address this kind of challenge. They don't take into account how access is used. Unfortunately, these solutions have been eclipsed in their standalone ability to manage identity and access effectively. The scale of unmanaged access often represents millions of entitlements that an organization must contend with. An influence which has contributed to this troubling trend has been Sarbanes-Oxley requirements, resulting in the unsound practice of rubber-stamping broad swaths of account access certifications and the practice of access cloning. As a result, excess access has become institutionalized, a default, yet risky, organizational process.

Years of investment in traditional security approaches have not improved the outcomes. The CyberEdge Group's *2017 Cyberthreat Defense Report* states that 79.3% of organizations were breached in the 12 months before the survey, a distinct rise over the preceding year. This represents a disquieting and rising upward trend. Yet with the factors described above, what are security teams trying to detect? Known bads? Or unknown unknowns?

Meanwhile, *CSO* magazine observes organizations are unable to keep pace with the dramatic rise in cybercrime and are a refocusing their defenses from PCs and laptops to smartphones, mobile devices and billions of under-protected IoT devices. This has prompted estimates of spending for security in the range of one trillion dollars between 2017 and 2021. Organizations find they don't have all the tools they need to assure the security of their environments. What's required is an ability to tighten the identity access plane that modern attackers are leveraging through phishing and other forms of social attacks. The discovery gap of unknown privileged access entitlements must be closed with the awareness gap of how access entitlements are being utilized for an effective identity and access management program. As well, an integral part of the risk management strategy should include an ability to provide visibility into all instances of access entitlement, to monitor what access is being provided, how it is being used, and to have the capability to assess those instances with timely and reliable risk-based scoring.

Security leaders should assume attackers are inside their networks and that they must be detected and shut down. The most effective way to detect them and to find high risk is through their behavior. What we need to be looking for, and *seeing*, in the future, is the unknown, most often from the inside. The question is: what is their behavior and what is the relative risk of that behavior? Yet within a growing sea of digital exhaust the scope of the challenge now lies well beyond manual human capabilities. Without a precise prescriptive behavior analytic solution, driven by advanced machine learning and drawing from big data for context – identifying inside threats in near real-time – the ability to identify and stop these attacks, only with human capacity, becomes simply impossible.

Now, in the wake of the 2017 Equifax mega breach – and following close behind, revelations of the troubling Security Exchange Commission (SEC) breach, where they were warned repeatedly about weaknesses in their security – the stakes have reached a critical magnitude. The need to identify unknown threats and risky behaviors is growing within the circles of forward-looking security leaders. This approach represents the only effective and realistic path to analyze the surface area of identity for access risk, while detecting behavioral anomalies from advanced machine learning baselining. We call this solution approach Borderless Behavior Analytics.

In this second edition of our book, we have added to the assembled thought leaders who are from a range of different industries – from financial services, healthcare, transportation, agricultural biotechnology, manufacturing, cutting-edge social media, government, hospitality and more. They have witnessed the changes in this landscape and have delivered solutions to address it. We share their experience, and their lessons learned, so that others following similar paths might benefit, and possibly avoid wrong turns. We also draw from industry analysts, leveraging as well, the deep bench of seasoned expertise at Gurucul, to share insights into how data access and use are changing, to offer a resource that might help assure the success of your organization's future.

By reading this book you're joining a journey of discovery which defines the evolving future of cyber security and the robust challenges of addressing access and activity risks. We hope to help make your journey a productive one.

Saryu Nayyar
CEO, Gurucul

1

Impact of Cloud and Mobility for Identity

The Evolution of Urgency for Change

So how did we get here? How did we arrive at this kaleidoscopic world of security challenges?

About ten years ago, the traditional chief information security officer's strategy for companies was to have a hard outside shell and a soft inside, something like an exoskeleton. This paradigm was established in the 70's and 80's. During that era, many mainframe set-ups maintained their data centers in central locations and built their security to protect these monoliths of data.

With the advent of technology developments in business that delivered more convenience and productivity, security teams were compelled to move to more of a distributed and open security policy. Business demanded that. Over the last six years, with the widespread use of the multifunctional mobile smartphones in business and companies experiencing the expanded BYOD (bring your own device) demand, the relevance and value of these original traditional security perspectives and strategies were coming to an end. Concurrently, the advent of cloud adoption had been expanding. A paradigm shift for security of this evolving technology was at hand.

> “*A paradigm shift for security of this evolving technology was at hand.*”

Cloud adoption first began as a shadow IT activity, beyond an IT organization's supervision. The trend started with small pockets of users using different software solutions that were easy to set up, and often free, to share files, instant text, post professional profiles, and more, (Box, Dropbox, Skype, LinkedIn, etc.) for their perceived advantages. These were completely outside IT's visibility. This usage took root across business units where employees resolved challenges which IT was unable to address in a timely, responsive manner, by accessing easily available cloud-based applications. Unsanctioned employee-driven IT had established itself in the business setting and this raised security concerns. While these solutions delivered enhanced productivity and flexibility, they did not focus on availability, scalability or security concerns. Then, a number of companies began to offer tools to provide visibility into what applications were being used within an organization's environment.

This ease of use and heightened efficiencies, however, led to expanded offerings and utilization of cloud applications. Organizations also witnessed groups within the corporate structure adopt top-down applications like Salesforce, with its sales force automation capabilities, to meet their business goals. This trend represented a growing migration for enterprise applications. Organizations would adopt a software as a service (SaaS) solution from the internet, the pattern of corporate adoption would expand — both within an organization and across the marketplace — eventually manifesting into the wide array of public and private cloud applications we see today. Migration of corporate information had moved outside the firewall, again without IT's official sanction. These popular cloud business applications included Zoho for enterprise business applications, as well as DocuSign for secure document signature management, and others, all delivering robust productivity within their specialized niches. The kaleidoscopic world of security challenges was well on its way.

Salesforce.com became acknowledged as the first widely adopted cloud business application. Their SaaS solutions originally offered portal access for different customers. Over time, they expanded and productized their solution to the point where it became a standard for sales organizations within a broad range of companies. More cloud solutions proliferated, offering new modes of productivity enhancement and other advantages. And as cloud gained in popularity, more and more data moved outside the perimeter.

In the recent past, organizations' adoptions of more comprehensive cloud solutions, such as Amazon Web Services, Rackspace, Azure, Office 365, Google Apps, and other cloud solutions, have subsequently become standards. Business was dictating to IT: "We're going in this direction." This wholesale migration began about five to seven years ago as business applications like this came into more widespread availability. At that point, with broad sets of data residing in the cloud, the question for security leaders was: "Is it secure?" Demands for assurance of security in this newly evolving IT hybrid environment moved to the forefront, and rightfully so. Today, trends reveal the growing preponderance of specialized cloud adoptions in larger companies, where 82% of enterprises larger than 1000 employees have a multi-cloud strategy, with 71% hybrid cloud (*RightScale 2016 State of the Cloud Report*), all trending up from the previous year.

One of the advantages that cloud solutions provided was that they did not have legacy application and infrastructure to integrate into their solutions and the majority designed environments with security built in from the beginning.

An early driver for establishing policies for security and the protection of privacy was the Security Breach Statute – California Senate Bill 1386 (SB-1386, July 2003). This was the first piece of major legislation mandating that if a company lost any customer information, and it was not encrypted, then the company was required to report it to the customer. The statute also stipulated that "*…any business that violates, proposes to violate, or has violated this title may be enjoined.*" So any enterprise representing themselves as being responsible for handling or managing sensitive customer information would be subject to a mandate requiring that customer information must be protected in a secure and standardized manner. Transparent and timely disclosure of any serious change in security status was a strict requirement. To do otherwise would be a risk for any business with paralyzing and costly legal sanctions.

The appearance of the chief information security officer (CISO) title on IT org charts, and the accompanying official roles and responsibilities, evolved in the early 2000's. The CISO's job was to protect a company's revenue producing business and the constituent sensitive pieces of data which support that objective. Yet with all a given organization's important data in the cloud, and with business applications on mobile phones, tablets, etc., being used 24/7 from everywhere, the burning question for security leaders had become: "How am I going to manage the risk with all these devices and applications — both on and off the cloud?" Data was no longer behind the firewall. That single security control point was gone. The border was gone. The data was no longer safe inside the fortress, because there was no fortress. The data resided in multiple locations outside the enterprise.

> ***The data was no longer safe inside the fortress, because there was no fortress.***

Since the complexity of this usage trend was often initiated by business leaders in organizations outside the chief information officer's (CIO's) sphere of responsibility, some CISOs found their mandate at cross-purposes, generally taking a reflexive 'Dr. No' position on these productivity enhancing innovations. Earlier, instead of threat hunting, the traditional security tools from five to fifteen years ago involved the process that would entail placing a constraint, but only if a potential threat was understood. Of course, if an organization shut everyone out, there would be no threat, but without access, the business operations would cease. Yet the challenge remained that "we don't know what's coming at us next" concern. Nevertheless, successful CISO's generally recognized the importance and value adopting a consultant and partner-like role with the rest of the business, and helping them understand what best practices were required to assure effective security in their rapidly evolving hybrid IT environments. That meant CISOs needed to raise their game and take responsibility for all the new complexities an enterprise was taking on, or considering to take on.

This brave new evolving and complex networking world has represented a serious challenge for businesses. At first, organizations provided limited transparency. Then, to comply with government mandates, security teams had to know if data had been breached. They needed to identify what tools they possessed to assess the magnitude and direction of a breach. Yet traditional firewalls and other security applications were all designed to detect breaches coming from outside of the network and via known attack vectors. They were weak at detecting threats emanating from the inside. Security information and event management (SIEM) solutions had delivered value for over a decade of centralized visibility, mainly for compliance and operations, yet only recently provided selected threat hunting capabilities. Intrusion detection systems and intrusion protection systems (IDS/IPS), as well as data loss prevention (DLP), were designed more for awareness, than protection, resulting in event and alert input into SIEMs for more context to lower the noise factor. These tools, however, could not address the persistent risk of malicious insiders, which security experts recognized was on the rise and showing no signs of abatement.

Several years of escalating breaches were delivering an alarming quantity of alerts, creating fatigue among security staffers, with far too many futile false positives. Declarative defenses were not managing the challenge. New attack trends could not be fingerprinted when they were analyzed, because many attack signatures were unique due to massive polymorphism. There was surge of cybercrime beyond the scope of signatures, patterns and rules in declarative defenses. The complete breakdown of the perimeter had become manifest. This sobering observation ushered in the realization among CISOs that they no longer had effective controls to address the urgent evolving challenge. They recognized that a serious systemic threat to their organization's livelihood was at hand.

This sobering observation ushered in the realization among CISOs that they no longer had effective controls to address the urgent evolving challenge.

Accentuating that realization of pandemic exposure, numerous events occurred between 2009 and 2012 that served to heighten security leaders' concerns, which included Operation Aurora and Stuxnet. Launched by a group affiliated with the People's Liberation Army of China, Aurora involved a series of cyber-attacks conducted against a host of American companies, including Google, Adobe Systems, Juniper Networks, Rackspace, Symantec, Northrop Grumman, Morgan Stanley and Dow Chemical. The objective was penetrating security and gaining access to the crown jewels of these high tech, security and defense contractor companies. Stuxnet was a targeted worm virus, alleged to have been developed by Israeli and U.S. groups. It was used to paralyze Iran's nuclear program by targeting Siemens computer systems which controlled Iran's nuclear centrifuges, of which one fifth were ruined. This event demonstrated that even physical assets could be compromised or destroyed (by changing the speed of the centrifuges) through cyber-attacks. The Stuxnet breach methodology also included leveraging four zero-day attacks, where just one zero-day exploit itself is highly valued. On a wider scale, a swarm of other zero-based events proliferated in the cyber world and continued to rise in frequency. A new alarming era of exposure had arrived.

Organizations saw that a new awareness and paradigm were required — a new way to look at, assess and strengthen the security of a business's crown jewels, their data. Sarbanes-Oxley certification requirements were in place. Earlier attitudes treated compliance reporting as an afterthought. Now, a number of larger organizations approached this requirement in a similar way service providers had with service level agreements (SLAs), a serious requirement of due diligence, giving this reporting a much higher priority. Conversely, some organizations sought to circumvent the meticulous requirements, and falsified their certifications. Meanwhile, enterprises recognized that intellectual property (IP) theft was on the rise from insiders. Cases included groups of employees and contractors at high tech companies, sometimes disgruntled, who moved to other companies taking their work with them, feeling unfounded entitled ownership of the intellectual property, despite employee contracts to the contrary. The complexity of exposure and risk for enterprises both outside and inside the organizational framework continued to unfold and amplify.

More recently (between 2012 and 2015), an evolutionary development of SIEM took place representing a functional amplification of the solution set, fortifying SOC's (security operations centers) capabilities with enhanced solution features such as the 'single pane of glass' concept, providing a centralized view of all system events and alerts. This further enabled forensic security capabilities that delivered insight into the pattern of an attack and how it happened. This meant SOCs could generate and manage their own threat intelligence. During this period, solutions like FireEye's advanced persistent threat (APT) detection appliances and sand boxes became more common. At this stage of security evolution, organizations were developing their own security intelligence, taking ownership of understanding the steps in the cyber kill chain (1-7) and developing a deeper awareness of how attack methods evolved. During this time, however, the declarative statement method to assess cyber security maturity was being challenged for the increasingly constrained value it delivered to security.

To respond successfully to this challenge, businesses needed to initiate a new perspective on the focus of identity, access and entitlements. Everyone should have their own ID, everyone should have their own set of permissions and credentials for the systems and

> *What was crucially different now, however, was the amplified view of the value of identity and access.*

applications they interface with. Otherwise, traceability would not exist. What was crucially different now, however, was the amplified view of the value of identity and access. Before, like compliance reporting, these elements were secondary in security priority. Now, they were becoming elevated to a crucial strategic role. How business and security viewed the role of identity and access in an organization defined how successful an organization's security strategy would be.

Yet, there was now too much data in the SIEM, and it was doubling every year. Any serious prospect of managing security analysis solely by human means was quickly becoming futile. Around this time, the misuse and compromise of identity emerged as a serious threat plane. Mismanaged with outdated legacy policies and rules, identity became an easy attack plane to compromise over-privileged accounts. Effective identity management was impaired. While its access enabling function remained important, its ability to actually see what identities were doing in the environment were piecemeal at best. Vast gray areas of activity anomalies remained unknown, and they were growing. Behavior was a blind spot. The behavior of activist insiders like Edward Snowden, and disgruntled employees, elevated the profile and visibility of the insider threat, highlighting the potential for severe negative impact on organizations. The perimeter was officially gone. A reliable new approach in security, capable of evolving with the changing environment was needed. This entailed effective behavior visibility and monitoring.

Identity and access are core components of a classification process to achieve the best method to define normal and abnormal user and entity behaviors. If a threat actor wanted to steal data from a network, they would need access to that data. The threat plane is comprised of identities and their associated credentials. That's the basis of access and the direct route to anything in an organization's network. With the evolving challenges, and sobering lessons learned with from recent high profile data breaches, the importance of identity and access was now better understood and perceived much more strategically by forward-looking security leaders. Security teams needed to know who was in their environment, what they had access to, and what were they doing there.

> *The threat plane is comprised of identities and their associated credentials. That's the basis of access and the direct route to anything in an organization's network.*

These undefined activities represented gray areas of unknown risk. Addressing this challenge requires a comprehensive, accurate and timely measurement of the risks that lurk in the uncharted gray areas. Within that requirement is a recognition that visibility of privileged access accounts and entitlements risk is at the forefront of concerns, because a majority of privileged access within an organization is simply unknown at the entitlement level and within applications. This risk-based assessment capability has undergone various phases of evolution, based on need, while harnessing state-of-the-art technology capable of developing and delivering next generation security monitoring.

The first generation of information security professionals was generally comprised of forensic investigators who could discover and define the kill chain. They thrived on solving the mystery of how a threat actor broke into their system, from where and what method was used, and then closing the security hole. Over time, however, as environment complexity and the number of endpoints grew, it became too cumbersome, time-consuming, and expensive, to do a deep security dive. In addition, this approach did not improve security teams' abilities to stop these attacks.

During this time, an industry-wide awareness of this challenge grew. By 2008, the Center for Internet Security (CIS) and the SANS Institute had been participating in a public-private partnership with the NSA. This ultimately expanded to a wider consortium, which included international participation to examine the problem more holistically. An important outcome of this initiative was refining a list of security controls (*CIS Critical Controls*) that were most effective in preventing known attacks. These controls were widely adopted and continue to be periodically revised, encouraging shared continuous diagnostic investigation. A new proactive security framework had begun to evolve, promoting a structure for constructive security. Prescriptive advice began to show up in the role of security, along with fundamentals of security hygiene and best practices. Recognizing the need to target identity and implement behavior monitoring had begun during this phase of security evolution. This requirement, however, would also need to address more complex environments, demanding the application of new perspectives.

A new risk challenge emerged — 'dwell time' — the average time between intruder infection and detection. It was far too lengthy, by industry estimates, with the average often exceeding 200 days, and currently estimated at 206 days. Attackers were spending months inside an environment undiscovered. SOC team effectiveness declined markedly, and became a major concern, even as new versions of SIEM were unable to improve the detection rate. Using a compromised identity, malicious attackers would move unimpeded, laterally, inside an environment. A risk-based solution was required to comprehensively address the myriad of challenges plaguing security teams dealing with account compromise and misuse, plus unknown anomalies based on access and activity in their hybrid environments. The era of user and entity behavior analytics (UEBA) and identity analytics (IdA)* security solutions had arrived, and none too soon.

Filling the gap of SIEMs, UEBA delivered identity-based behavior analysis of access and activity for new data sources including SIEMs, directories and applications with insight beyond what technical experts had previously been able to view with log access files. As well, IdA helped close the discovery gap of unknown access risks, with a special emphasis on the vast threat plane of privileged access. Now the prospect of preventing data exfiltration, detecting insider threats, as well as compromise and misuse of identity through phishing and social attacks, had become a realistic goal. These

* While IdA, as standalone class of solution, has been available for years from select UEBA vendors, Gartner Research coined the term in early 2016, identifying it as an essential component of advanced security analytics.

solutions delivered a new effective method to leverage and monitor an identity to establish what's normal and what's not. Finally, security analysts could answer, "What access risk does this user have? What activity risks does this user have?" and "What is the context of these risks?" This provided granular insight into how an identity's access and activity behavior was different from what their peer groups were doing, in all the different variables of: who, where, when, how, what action, and how these actions correlated with baseline definitions of established normal behavior.

The essential component of a successful and best-of-breed UEBA and IdA solution model involves machine learning. Drawing from big data for context, across all environments, machine learning delivers the mechanism to enable a broad range of issues to be managed, to find the red herrings, to discover what's going on and what's different or out of the ordinary. Advanced machine learning is designed to recognize that just because a behavior is different, it doesn't mean it's bad, and it eliminates potential red herrings from consideration.

> *...machine learning is designed to recognize that just because a behavior is different, it doesn't mean it's bad...*

Ultimately, a mature UEBA-IdA solution would furnish businesses with a centralized easy-to-use single view that encompasses all the users and entities in the hybrid environment. UEBA then provides holistic monitoring of access and activity where various levels of users and solutions leverage prescriptive risk scores to reduce access risks and detect unknown anomalies. While SOC teams will likely leverage risk scores within a UI, bidirectional API integration with solutions enables risk scores to drive automated risk responses. Forward-looking organizations finally have a cost-effective, efficient and reliable approach to address the urgent security priorities in their global environments, 24/7.

In this brave new world, there are, of course, early adopters who have traveled the road of integrating UEBA and IdA solutions and faced the challenges they represent. Each organization and industry segment has their own influences, challenges and requirements. In this book, we are proud to present to you CISO leaders from a range of business sectors who share their own insights and experiences on the UEBA and IdA journey through Borderless Behavior Analytics, facing the challenges of today's new evolving hybrid IT environments. They also discuss their strategies, goals and objectives of next-generation-facing UEBA and IdA solution requirements.

While the introduction and this chapter position UEBA and IdA via machine learning from the context of big data as an answer to cyber security challenges, the journey in the forthcoming interviews is rich with wisdom and experience beyond any possibly perceived promotional partiality.

Our first expert, Gary Eppinger has served in a broad range of industries, and arrived at a setting he calls a 'hyper-hybrid environment'. The challenges he has faced are unique, and his perspectives on the solutions required to address those challenges draw from his extensive security experience in a number of different vertical markets, from finance, manufacturing, retail, health care and more.

BORDERLESS EXPERT INSIGHTS

Gary Eppinger, CISO *
Carnival Corporation

Global VP, Chief Information Security and Privacy Officer for Carnival Corporation, Gary Eppinger conceives, implements, and leads technology solutions that protect corporate assets, increase organizational capability, and advance productivity for Fortune 100 companies. He is recognized globally as a highly valued resource with an exceptional ability to build and develop IT teams that deliver critical business objectives in companies within transformation. Ranked 24th in ExecRank's "Top Security Executive Rankings," Gary is an active speaker on IT and cyber security. He also assists numerous companies serving as a valued board advisor.

A member of Gurucul's Board of Advisers, Gary has provided valuable guidance in the company's evolution through the complex path of challenges facing the company's emergence in the field of UEBA security. He shares some of his seasoned in-depth insights into the challenges of hybrid cloud security and behavior analytics' place in it.

Overview

Eppinger begins with his observations on how data access is changing today's environments. He provides insights on the symptoms that reveal security defenses are a problem today, and then discusses the business vulnerabilities of a compromise leading to a breach. The critical drivers around the importance of insider threats are examined, as he notes the growing concerns about privilege misuse. Drawing from his unique Carnival Corporation experience, Eppinger shares insights on the impact on security defenses with a constant flow of insiders and customers traveling on ships, to land locations, or in combination. This systemic view incorporates environments around the world, across different on-premises locations, in the cloud and on the sea, and includes the profound impact on this exceptional hybrid environment's security requirements. The new role of identity-based access and activity risks, and how they tie together, are explored along with the key solution components required to address the needs of constantly changing security conditions. This topic also expands into the handling of the vast and growing scale of data for security analysis. Eppinger shares his perspectives on machine learning and predictive security analytics adoption in the environment and within his industry vertical. Finally, he provides his distinctive perspectives of security evolution through the wide range of vertical markets he has worked in which has shaped his approach to work in one of the most complex hybrid environments imaginable, something he calls the 'hyper-hybrid environment'.

* The views and opinions expressed by Gary Eppinger in this book are his own, and do not necessarily reflect those of Carnival Corporation, or any of his previous employers.

How data access is changing today's environments

Carnival Corporation's strategy for managing data has changed over the last few years. Originally, we were primarily a corporate holding company. Each of our ten brands was a standalone cruise company which we ran independently. They competed for customers internally, as well as with external competitors. Carnival just happened to acquire them and put them under the same umbrella.

Separate siloed views of data. This meant from a data perspective that corporate and customer data, the fuel of the company, was separated and isolated from each particular brand. For example, the information on customers for Carnival Cruises, AIDA, and for Princess, were all stored and accessed independently. When Gary Eppinger cruised on ships from all three lines, we were only capable of seeing that information associated with him separately, in each silo of data, with no correlation whatsoever.

Phased migration to a centralized view. We have worked to concatenate and bring that critical data together in phases, and over the last two years we acquired two more of the consolidated views of our customer data. This means if I am a customer of all three of those brands, corporate Carnival can now see all this in a single repository. As well as that, we market to customers differently because we can now correlate and use this information effectively and have insight into the preferences a customer has established on any ship and cruise line. More consolidated cruise brand views are in the works.

> ***We have worked to concatenate and bring that critical data together in phases...***

Centralized identity value. An example of the advantage this new visibility provides is if I sailed on Carnival fifty times, Carnival has a great deal of value data and information on me as a cruiser. When I go with Princess and Costa one time, I may look like a new customer to them, with no history. Now we can add visibility into these fifty Carnival cruises. They now know what food I like, they know if I'm a spa person, the types of spas I prefer, and the types of rooms that might make sense for me. So my identity represents great value information that can be leveraged to make my vacation a great experience.

New capabilities in risk management. As we bring that data together, it also gives us more of a capability to detect a higher level of risk to the information. As the data becomes concatenated into a single place, we know more effectively if it's compromised, a higher risk, or not protected properly. When it was spread between ten different brands, and two hundred different locations, it was much harder to get to and monitor properly. Now that it is coming together, it also raises the bar of what we have to do to protect that information.

The symptoms revealing security defenses are a problem today

No longer is it an environment where a CISO might have fifteen branches and a fixed number of connections, along with access and users connecting into their environment. That was manageable then. Today, however, there are millions of customers, millions of entry points, millions of devices connecting into our environments all over the world. That's millions of connection points we're responsible for. Now it's no longer possible to rely only on the entry point into our network, into our environment, to provide security assurance.

> *Today... there are millions of customers, millions of entry points, millions of devices connecting into our environments all over the world.*

Moving security closer to the data. Generally the closer you can put your controls to the data, the better you are. If you think about the traditional approach CISOs took for the last twenty plus years, we originally built the walls as far as we could from the data, just at the network layer, and then this model was no longer viable. In response, the focus moved to the application layer and data was controlled at the ERP (enterprise resource planning) level with multiple applications together. Finally, the objective became to move the security focus to the database level.

Maintaining the right controls on data. Today, it's a multi-tiered approach where you need to have appropriate controls across all the different channels and/or layers to make sense. Yet at the same time it includes sustaining the objective of maintaining controls much more closely to that data, no matter where the data resides, as well as how that data flows and where it flows to. Some of these controls need to go along with the data as it moves to its destination because data does not reside within the servers of an isolated DMZ all the time. It's continuously being leveraged, moved and adapted from system to system. In addition, you need to think about your controls based on location or point of time.

Technology evolution and new security perspectives. With technology and data use patterns continually evolving and changing, the old strategies of manual security monitoring have become unrealistic. This clearly indicates that an era of information security has passed and that the new age will require entirely new perspectives and solutions on how to achieve the same original goal of twenty years ago: to protect the information.

> *This clearly indicates that an era of information security has passed and that the new age will require entirely new perspectives and solutions... to protect the information.*

Security driving business value

Carnival protects a great deal of critical information — from credit cards, passports, driver's licenses, to health records, and more. This, of course, includes massive amounts of critical information for a huge number of customers who sail with us every day. Millions of customers entrust us with that information because it's essential for us to be able to deliver a high quality vacation for them. We take this responsibility very seriously. The prospect of damaging that trust represents a threat to our brand reputation. Without our brand reputation, customers' loyalty erodes and people simply choose other vacation destinations.

A range of security concerns. Anything that could damage our reputation is, of course, a serious matter, but data exfiltration, customer hacking, or customer information threats are all top priority critical concerns for us. We also think about safety and security at the highest level of importance to the company and to our employees. From our perspective, in an industry which services so many customers traveling through the world, our focus includes anything that involves the physical safety, or the perceived safety of an individual. Anything that might harm a customer, or one of our employees, is a foremost concern and priority. Therefore, any issue that could create a question over whether someone might somehow be physically harmed is paramount. This is all part of our DNA. It's part of what makes us successful and differentiates Carnival.

The focus on financial protections. Following very closely, of course, is the mandate to protect against any kind of financial threat. Here, the range of risk, which could translate into financial threat, is varied and wide. The theft of money itself, the theft of IP, the misuse of assets that incurs financial damage, and brand damage, are all part of this perspective. This expands to include other concerns as well, such as protection of onboard medical records and more.

A broader set of requirements than most enterprises. In addition, any issue concerning the proper running of our ships and the systems that control them are also our concern. This includes the medical centers, navigations systems for the ships, the computerized operations that run system safety checks and all those unseen processes that are taken for granted by the public. These remain our sacred trust to ensure their integrity is assured. The scope of security responsibilities for us is much broader than traditional land-based corporations. It's what I call a 'hyper-hybrid environment'. Within this complex world, the core essence of our information security mandate is: protect your people, your information and the finances.

Facing the prospect of insider threats

Businesses run on the concept of entrusting their employees to do the right thing with their access to the environment, access to the data, and access to their customer's data. It's been said many times: employees are our biggest assets and are our biggest risk exposure — so insider threat is a big deal to us. Of course, it is often the case that an outside threat first appears as an insider threat to a security analyst because of a compromised identity. However, either way, these people may be using the data inappropriately, not for its intended use, nor to the benefit of the company or our customers, and quite possibly to the advantage of our competitors.

> *…it is often the case that an outside threat first appears as an insider threat to a security analyst…*

A range of risk from breaches. The serious damage from insider threats can impact any and all of the areas of business vulnerability. These include brand reputation, customer trust, along with liability, loss of position in the market against competition, or fines, and the list goes on from there. While protecting the financial well-being of Carnival is a top concern for us, along with the well-being of our customers and our employees, the potential of an insider breach remains an equally important security mandate.

Growing concerns about privilege misuse and compromise

Privilege misuse is an issue that scares me relentlessly. This is especially the case with employees who have the higher privileged accounts and capabilities. As my colleagues in the UK say, it's "The Keys of the Kingdom" – and that's the last place you want the bad guys to be able to get to. From there, with the right HPA (high privileged access), and without the right safeguards in place, they can exploit your environment with impunity.

> *…it's "The Keys of the Kingdom" – and that's the last place you want the bad guys to be able to get to.*

A fundamental security requirement. Understanding where those accounts and entitlements are, how to maintain them, how to restrict these privileges, and how to limit the risk and exposure, is critical for every company, no matter what their size. These proficiencies must be fundamental capabilities from the security perspective. In addition, as we expand our utility of predictive security analytics and machine learning, enhancing and empowering these objectives for our HPA accounts, security is at the center of our priorities to achieve.

The hyper-hybrid security environment: A constant flow of insiders and customers on ships, land locations, or in combination

The security of our hyper-hybrid environments must be adaptable to these different changes of user behavior based on location, on high volume, or based on need. We're in the process of implementing a long-term strategy to enhance our identity capabilities to be able to meet these new demands; it's a high priority.

A single view of identity is needed. Our employees and customers are included in this planning where their identities must be managed at a much higher level, enabling a holistic unified visibility of the individual. It's a highly complex challenge, especially with our customers. As a model, consider the type of individual who has one or two banking accounts, a car loan, and credit cards. They have multiple financial companies that they deal with every day, all with different identities. All must be managed separately. That's very complicated, even for individual accountability. So how do you do this across multiple companies within a corporation? Resolving this challenge is our objective.

The complex journey to achieve a single view of identity. While we may have the same customer on our different lines, we do not yet have the singular centralized view of them, and this is where the industry is going. From the Carnival corporate perspective, with our ten different companies, we are working through phases to achieve that goal, most recently with the first two consolidated brands clustered and migrated into a single view. It's important to understand where it all began as well. We've made decisive strides away from the time when cruisers sailed with all ten different companies, and would have ten different identities, which had ten different configurations, forcing Carnival to interface with you as a single person in ten different ways. Our ultimate path forward will be a single path, a single way of managing this as a single identity across all environments. The magnitude of all this information, originally residing in ten separate silos of different architectures and levels of maturity, is a considerable factor of the challenge.

The impact on hybrid environment security: Systems around the world, on-premises, in the cloud and on the sea

One of the things we talk about as we look at our security model, and strategy, is the level of maturity in our security capabilities, now and in the future. In doing so, we try to maintain as realistic a perspective as possible when we talk about what solutions we need in place to assure security in the future. We also know once we get there, because of the rapid evolution of technology and the cloud, that it will probably no longer be completely adequate.

A realistic view of phased progress. With this understanding of constant evolution in technology, we don't need to take a solution to what some might consider an ultimate world-class level. We do need take it to a level of reliable functionality. With that perspective, we maintain the strategy of continuous development and improvement, not adopt some monolithic solution that might be outdated as soon as it is finally implemented. For security, solutions must be light and flexible, capable of evolving in the same way, to integrate and grow with the various phases, and with all the complex variables. This is where user and entity behavior analytics and identity analytics represents the potential for productive growth with us at Carnival.

> *...we maintain the strategy of continuous development and improvement, not adopt some monolithic solution that might be outdated as soon as it is finally implemented.*

Integrating analytics and machine learning through phases in the environment. Of utmost importance, we have focused on the level of complexity required to move a global organization, which has data and information, as well as processes on-premises, off-premises, at sea, in the cloud, and across ten different brands. These were originally at different maturity levels, along with the varied applications, systems and infrastructure. From the start, we've dealt with a massive level of complexity. The goal we maintain is to drive the unified maturity of all our brands, to that same level, no matter where the data resides. This is especially true now that we have so many different places we have to be monitoring to assess risk and assure security. As we consolidate our views of the different businesses, machine learning is part of that integration process, which provides a strengthening of defenses at each phase by identifying risks and unknown threats.

Robust machine learning required for comprehensive security. It boils down to that old adage; we are as strong as our weakest link. If we're strong within the on-premises, and the cloud protection is weak, then we're collectively weak. If we're strong within the on-premises, at corporate offices, but weaker on the ship, then we're all weak. How do you identify that weakest link? As we view the challenges holistically and consistently across all of our stationary environments, as well as the constantly moving elements of our global environment, this is the focus of our strategy. Because of this wide-scaled environment, with increasingly high data volume to analyze, we needed big data and behavior analytics to find those weak links.

> *Because of this wide-scaled environment, with increasingly high data volume to analyze, we needed big data and behavior analytics to find those weak links.*

Adjustments required to assure security in hyper-hybrid environments

It was a challenge for me to adapt at first. As a traditional professional who believed in risk management, and in the security principles that developed over so many years in the space, experience in the evolving complexities of the hybrid world has shown me a new reality. This is not an uncommon realization for CISOs to experience today.

A new normal of viewing security. I now have the perspective of, "It's not *if* I get compromised, it's *when* I get compromised." More importantly, upon reaching that recognition the priority then quickly becomes, "How do I determine exactly when it happens so I can react in the most efficient way to bring the environment back into compliance and ultimately stability?" These priority concerns center on resiliency. Keep in mind, you still need all of the preventive controls discussed earlier, but you also need the balanced detective and responsive controls in place as well.

Strategies for strong recovery following a breach. Because of this new perspective on today's security realities, we've changed our paradigm. We're no longer saying "if". By implementing a prescribed selection, along with a number of controls and declarative defenses, we know certain security events are managed. Yet, now we're also saying that when it happens, how do we know it happened and what was the magnitude? That's critical to know the extent of the compromise and the proper remedial steps required to prevent further attacks of this nature. This also leads directly to how we react to that breach as it is happening and bringing the system back into compliance and a maintainable state as quickly as possible.

The new role of identity and access: How they tie together

Identity and access have been around since the beginning of network security. However, that essential commissioning capability companies have had in the past must migrate to a higher level, delivering security assurance and enduring value. CISOs begin with the perspective that they want to assure their employees, contractors, partners, customers, and vendors, have the right access at the right time. This includes no more access than is required, with access ending when it is no longer needed. This is a fundamental business objective and absolutely important. But if you think about an employee – or a customer – along with their lifecycle of access requirements, they have changed. The access control objective hasn't changed. What has changed is our ability to assure the right access at the right time, at the right location, based on legitimate need.

Perpetually fluctuating user access. Specifically from the employee perspective, an example of the challenge is we have a range of accountants with Carnival Corporation. One may be working on one of our ships, and their use profile and requirements might be distinctly different from an accountant who is working in our corporate office. Then we might have an accountant who is traveling from the corporate office, or to Asia, or is onboard one of our ships. Their access life cycle might be very different, as well, and may change periodically, based on their legitimate work role requirements. The challenge becomes how we make sure they have the right access at the right time. Of course, behind all of that is the need to assure the right person has gained that access.

Risks with limited visibility into a wide range of users and access requests. The variables of these circumstances are accelerating or deaccelerating perpetually based on the needs at a particular moment. That's where serious risks occur. If you don't know who your users, your employees, and your customers are, then you have no chance of ensuring you're giving the right access at the right time. Multiply that user environment by the amount of employees, partners and customers, and the magnitude of complexity and risk reaches staggering proportions. It's this next layer of identity that determines the importance of solid solutions for access and identity that are essential to the success of security.

> ***If you don't know who your users, your employees, and your customers are, then you have no chance of ensuring you're giving the right access at the right time.***

Key solution components required for constantly changing security conditions

Elements we have initiated include identity lifecycle management tools with the ability to integrate the identity in the cloud, versus on-premises, versus any one of our environments. The other initiative we are integrating is machine learning analytics capabilities and tools. We have also flattened our network from an active directory perspective. We originally had many active directories and then integrated them into one, flattening the network down to a single tree. This makes it possible for us to have complete individual visibility.

A challenging orchestration of solution elements. We're also working on embedding role-based security principles into our strategy from an identity perspective. However, the challenges continue as we investigate how we integrate the entire application layer. Incorporating application security and application capabilities into our roles, and into our identity manager, are key objectives for us. Those are some of the solution elements we are leveraging to give us a heightened level of capability so we can connect them gaining optimal visibility and controls. Without machine learning, none of this would be possible.

Handling the overwhelming scale of entitlements for identity management and security

Dealing with the huge scale of big data is the ten million dollar question for us. There's an evolving challenge with scale we've seen building over the last several years. Traditionally, we try to develop our solutions from a people, process and technology perspective. The days of just throwing people at a challenge to solve the problem are over, especially for companies with our size and complexity.

The staggering scale of big data. When organizations continue to adopt cloud solutions to improve their business flexibility and amplify productivity, they generate huge amounts of data to sift through – the digital exhaust of big data. From the complexity, size and demand perspectives, it's dramatically more complicated. We need to process increasingly larger amounts of data that must be adjudicated quickly in order to be able to get answers and to insure we're providing the right visibility for access as needed. This requirement can no longer be guaranteed through manual processes. That puts the organization's welfare at risk.

> *This requirement can no longer be guaranteed through manual processes. That puts the organization's welfare at risk.*

Traditional approach does not scale for complexity. Running security analysis, threat hunting and manual efforts on growing amounts of data in the traditional way becomes exponentially difficult. Add to that an identity perspective and there is simply no realistic way enterprises can scale internally to these demands. There needs to be a drastic game changer. It's something where you must leverage the cloud, big data, and machine learning with predictive security analytics solutions that include UEBA and IdA models and use cases.

The equalizing impact of UEBA and IdA. With a balanced approach of people, process and technology, woven together, we're driving to address the scalability problem that is growing faster than we ever imagined. We see all three of these elements coming together with cloud based providers that help us from the perspective of scalability. That's where solutions like UEBA, integrated with IdA, can help level the playing field for customers like us. UEBA and IdA combined is easily capable of running on this kind of a scale, with productive and actionable risk-scored results.

> *...we're driving to address the scalability problem... That's where solutions like UEBA, integrated with IdA, can help level the playing field for customers like us.*

People, process and technology benefit from UEBA and IdA. By using this solution, technology organizations leverage the computational capabilities of machine learning drawing from big data for context. This helps in terms of scaling, addressing security and identity challenges. From the perspectives of analytics processing, the systems are running more efficiently with fewer false positives. From the people perspective, the highly qualified security analysts are being freed from time-consuming manual investigations and able to focus on higher business critical tasks supporting the evolving needs of the security group. UEBA and IdA change and adapt the business process in a measurable way, integrating and optimizing a combination of people, process and technology.

How past behavior is predictive of potential future anomalies

When monitored effectively, some past behaviors provide a great indication for predicting future security issues. Timely, accurate data and context are the key. Yet because of the vast amount of data in today's environments, it can't be processed effectively without the robust reinforcement of machine learning. With that enhancement supporting the analytics, we have much more data that can be processed properly to deliver the all-important context which enables us to understand more of those future predictable scenarios with anomalies that arise. These anomalies will be undetected without the analysis of large amounts of data made possible by machine learning.

Increasing quality of results over time. The potential to uncover those anomalies through user behavior analytics will increase over time. First, the bigger anomalies and some of the obvious ones will surface. But as the learning process refines, and the baselines become more comprehensive, that number will double and triple six months or a year from now. Five years from now this number will be increased by a factor of five hundred. As we and the machine learning solution continually learn, we connect more of the dots. We continue to improve the evidence, and with it our ability to accurately predict at an increasingly specific level.

Identity management in a silo. We must assure the issue of identity is properly addressed. Too often, identity management from a security standpoint is in its own siloed IT framework, separate from security. A result has been that many times in the past organizations would perform certifications in separate systems. They would be unsuccessful in identifying anomalies, as they would possess an extremely limited visibility of the access risk plane.

> *This is often access that was in fact there, sometimes for many years, but because of the siloed segmentation, it was invisible.*

Un-siloed identity is critical for useful analytics. When you flatten out the environment and examine this entire big behemoth of access data, then you can recognize the need to focus on identity, and then from there run identity analytics on the data. This will give identity access management teams a much richer context, where they can pick out the excess access and access outliers which otherwise go unnoticed. This is often access that was in fact there, sometimes for many years, but because of the siloed segmentation and human effort, it was invisible.

Machine learning adoption in the environment and industry verticals

It's interesting how some security people used to look at analytics very narrowly where they would have to come up with a rule or a query. This is great if they know exactly what they're looking for. However, this reliance solely on rules and queries limits security assurance and misses the critical issue of the unknown unknowns. Security analysts can't possibly think of all the ways an attacker might try to get into their environment. While they may try to think from their attacker's perspective, they can't reproduce every scenario. They have to be right every time, while the attackers only need to be right once. That's why user and entity behavior analytics and identity analytics are critical in today's environments.

Big data and machine learning lowers false positives. We're comparatively early into the adoption of machine learning. We're learning from some of the initial successes. First, we needed to confirm how well the solution characterizes normal behavior and then see how well we could detect abnormal behavior. The more we learn, the better we understand the wider capability of leveraging user behavior analytics to take us to the next level and understand how much of the detection would be false positives. We're improving on filtering the false positives as we get deeper context from our peer group baselines and mining the big data more effectively.

> *We're improving on filtering the false positives as we get deeper context from our peer group baselines and mining the big data more effectively.*

Analytics and machine learning models of other verticals. If you examine some of the early adopter industries, such as banking, their models show us the immediacy of what we'd like to have in our environment. For example, my credit card gets used in three different locations all within two minutes and my cell phone goes off. This is the kind of analytics capabilities we're working to achieve for security controls that match the quality of that particular customer process. These other vertical solution capabilities are continually evolving. Today, there are probably fifty different scenarios which are triggers for the banking space that they didn't have two years ago. We intend to achieve the same kind of growth potential in our predictive security analytics solution within our own unique vertical.

Adoption trends for machine learning within the cruise line vertical

From a cruise line perspective, we're beginning to see early adoptions. The industry is recognizing how the unique challenges of their hyper-hybrid environments require unique solutions. With complex environments along with the element of ships constantly in movement around the world, hosting a range of technologies and users – some of it going through satellites — advanced security analytics is a solution that fits with their needs, goals and security objectives.

Visibility delivered with each integration phase. Specifically with Carnival, we're still in the early design and implementation of bringing all of our systems together into this integrated environment. We see huge upsides for us. We're now able to do things that previously would have taken us weeks, if not months to accomplish, or we couldn't do at all in the past.

Perspectives of security evolution through a range of verticals

After working over twenty-five years in a range of verticals, primarily with a security focus, my career path brought me to Carnival. Originally beginning as a programmer analyst for the Federal Reserve Bank of Cleveland, my work involved disaster recovery of systems, including old mainframe security systems, before moving into IT security. Positions in steel manufacturing, and healthcare with Blue Cross Family followed. After working in healthcare insurance, my work in the field led to medical imaging products manufacturing for GE HealthCare, where my responsibilities included building and managing a global security team. During that time, my portfolio broadened as the quality leader for the corporation responsible for Six Sigma across the global organization. Finally, just before joining Carnival, I held the CISO position at SuperValu, a large distribution and retail conglomerate grocery store chain.

Carnival hosts an array of businesses in one model. My position at Carnival is unique in that the organization contains a multitude of businesses that I worked within through the years, as well as a few new ones. Carnival is many things. It is like a corporation with a collection of small floating cities. It is a conglomerate of a huge supply chain organization, a transportation/people moving business, a hotel, restaurant and entertainment services enterprise, and a retail store chain that sells product all over the world. We have the largest collection of casinos afloat and a dedicated casino vertical. Carnival also has a medical services component. All of our ships have medical clinic centers, which carries a security perspective for the protection and control required for the clinics and their healthcare records.

> “*Carnival is many things. It is like a corporation with a collection of small floating cities.*”

A global operation with thousands of customers. Carnival has the traditional physical environment, with the corporate offices needing to protect IP. In addition, our security model must include some of our ships with over 4,000 customers and 1,000 plus crew. That translates into over 120,000 employees, of which 70% are on the ship at any given day, across the world, versus traditional corporate offices with locations that don't move. Add to that our responsibility for over one hundred ships around the world, all with moving data centers, which also need to be able to run off satellites when far off shore. It's a new layer of complexity of how to deliver IT services specifically to the customer as well as to the employees who run the ship.

Witnessing the road of security evolution with big data and machine learning. As I have witnessed the trends in the security industry evolve from the traditional on-premises to the hybrid cloud, and on to what I call Carnival Corporation's hyper-hybrid environment, I have come to recognize and appreciate the continuous state of evolution and development required to keep pace with the challenges, the new threat planes and development in technology. For the foreseeable future, predictive security analytics and machine learning driven by big data will be part of that evolution.

CONCLUSIONS & TAKEAWAYS:

Recognizing the urgency for change in security

Gary Eppinger's hyper-hybrid environment is a unique model of security challenge, contending with the complexities of environments on-premises, in the cloud, at sea, and in constant motion. Any one of the separate business verticals within Carnival Corporation's multifaceted umbrella environment would represent a full slate of demanding responsibilities for many enterprise CISOs. As Eppinger improves his security environment, and concatenates his company's ten brands into one view, along with developing the required security solutions to wrap around his hyper-hybrid environment, he observes the importance of maintaining flexibility with growth, and phased solution evolution. This contrasts with some monolithic solution approaches that entail 'rip and replace' which are often outdated upon completion of implementation.

Balancing people, process and technology, Eppinger calls out the objective of achieving reliable functionality over perfection with each phase. Perfection is virtually impossible to achieve since technology is perpetually evolving. This phased strategy includes the integration of risk-based predictive security analytics and capitalizing on the short-term benefits, while refining the long-term goals and increasing the critical mass of quality over time. Eppinger's objectives include bringing unique and separate siloed environments under one centralized management approach. His strategy also includes moving security closer to the data itself, with the right controls.

At the core of this strategy is the holistic need for centralized identity, which optimizes the capabilities of risk management through robust identity analytics. None of this would be possible without the implementation of machine learning to leverage the burgeoning scale of big data in today's evolving hybrid environments.

The devil, of course, is always in the details. To achieve their security goals, security leaders must constantly update their understanding of a broad range of factors, including the importance of emerging trends in the misuse and the compromise of identity to keep in pace with their responsibilities for Borderless Behavior Analytics. This will be explored in the next chapter. For some high tech executives, however, an understanding of security risks should not be taken for granted. We'll see this in the following *Borderless Breach Flashcard*. These one-page case studies featured at the end of each expert interview section highlight the wide range of breach scenarios that security leaders face in protecting their evolving environments today.