Cybercrime Business Models: Developing an Approach for Effective Security against Better Organized Criminals

Charla Griffy-Brown
Graziadio School of Business, Pepperdine University

Demetrios Lazarikos
Blue Lava Consulting

Mark Chun
Graziadio School of Business, Pepperdine University

Cyber criminals and online criminal gangs are malicious actors with new business models. Today's cybercriminals are well organized, business savvy, and developing advanced techniques in exploiting organizations. They combine social engineering, viruses, trojans and spyware with sophisticated profit models, business plans and organization. This study addresses the following research question: What are the emerging cybercriminal business models and how are cybercriminals generating revenues? We will answer this question using qualitative and quantitative methodology exploring recent exploits, through executive interviews and independent evaluation. This paper will evaluate the business models that emerge using a validated business framework to score and explore the sophistication of these models. We will also share how business leaders can address these growing concerns.

INTRODUCTION

Cybercrime is increasing in velocity and reach touching all industries and verticals. No locale, industry, or organization is safe from attackers who wish to compromise their data. Verizon's 2016 dataset illustrates this point (Verizon, 2016). This year's incidents occurred in over 82 countries across a variety of industries, especially in the public, entertainment, finance, and information sectors (Verizon, 2016). There were far more security incidents than data breaches, or security incidents which resulted in the confirmed disclosure (not just potential exposure) of data to an unauthorized party. Phishing is a quick and easy way for attackers to steal a victim's credentials, which might explain why in 81.9 percent of incidents, the initial compromise took minutes (Verizon, 2016). By contrast, exfiltration took days in more than half (67.8 percent) of cases, a period of time which reflects a rise in point-of-sale attacks where malicious actors drop malware that capture, package, and execute scheduled exfiltration reports (Verizon, 2016). In 2015, there were 9,576 phishing incidents, 916 of which reported a breach of data. The main perpetrators behind last year's phishing campaigns were organized crime syndicates (89 percent) and state-sponsored actors (nine percent) (Verizon, 2016). For the first time in the history of Verizon's DBIR, the topic of credentials received its own section. There were 1,429 incidents of credential theft last

year. In those instances, attackers made off with credentials via hacking and malware, and they in turn used the stolen credentials more than three quarters (77 percent) of the time. (Verizon, 2016).

Importantly, not all vulnerabilities were exploited the same. Some flaws found in Adobe and Microsoft were exploited in a matter of days, whereas attackers waited months to exploit bugs in Apple and Mozilla. On average, bad actors took about a month to exploit a vulnerability, with half of all first exploitation attempts having occurred within a period of between 10 and 100 days (Verizon, 2016). This didn't mean attackers focused in only on new vulnerabilities. Quite the contrary, older vulnerabilities still proved to be a favorite tool among malicious actors. Some attackers also automated the delivery of weaponized vulnerabilities across the web (Verizon, 2016).

What is evident from an analysis of these security incidents and breaches is that there were a growing number of denial-of-service attacks across all industries. Web apps accounted for the greatest number of confirmed data breaches, particularly in the finance, information, entertainment, and educational sectors. There were also patterns commonly classified as incidents as opposed to confirmed data breaches (Crimeware, Insider and Privilege Misuse, and Physical Theft and Loss) which occurred mostly in the public sector and healthcare. This data contradicts the commonly held notions that cybercrime is focused on stealing credit cards and is a result of individual activity. Robert McCullen, CEO of Trustwave, a cybersecurity firm pointed out in their annual report (Trustwave Global Security, 2016), "Cybercriminals have been congregating and organizing for years, but 2015 showed a marked increase in the behavior we would normally associate with legitimate businesses."

These trends raise significant questions that business leaders and decision-makers need to consider: What are these business models? Are there trends and themes? Based on a clearer understanding of the evolution of cybercriminal activity organizations can begin to develop more sophisticated approaches to calculate appropriate risk in business initiatives and develop models for addressing an attack. This analysis will identify developing business models and their revenue streams. These models will then be analyzed using a business model framework to reveal broader themes and if they are sophisticated enough to truly be evaluated as a legitimate business model. We will also consider their impact on risk and mitigation. Based on this evaluation, we will present a risk-based approach for securing an environment without a perimeter against increasingly organized criminals.

THEORY AND FRAMEWORK FOR ANALYSIS

This paper proposes a different way of thinking about security with the growth of agile data architecture and the rise of organized cybercriminals. Agile data architecture has arisen with the opportunities available through cloud computing. Cloud computing is an IT enterprise architecture that continues to gain broader adoption. In legacy architecture solutions, the IT services are under local physical, logical and personnel controls. Cloud computing moves the application software and databases to large data centers, where the management of the data and services is controlled by a third party. This unique attribute poses many new security challenges for companies and opportunities for cybercriminals. Importantly, it opens up new business models and revenue streams for organized criminals – beyond just stealing credit card information or data. However, it is important to note that it isn't just architecture that has evolved but the cybercriminals themselves who exploit opportunities across traditional and agile architecture. We focus on applying recognized business evaluation tools for evaluating the strengths of the business models cybercriminals are using.

The cloud-security literature research primarily focusses on requirements and solutions for requirements (Honer, 2013, Griffy-Brown, et.al., 2016). In this regard, research on Attack/Harm Detection is prolific (Chonka, et. al., 2012; Chonka, et. al., 2011; Monfared, et. al., 2011). Non-repudiation is a topic widely addressed Nishikawa, et. al., 2012; Kumar et. al, 2011; Chou, et al, 2011). Security Auditing is also a topic that has been examined from a number of research perspectives. (Deshmuckh, et. al., 2012, Griffy-Brown, et. al., 2016; Munoz, et. al., 2012). The most researched topics in cyber-security are privacy, confidentiality, access and control (Chen, et. al., 2013; Cho, et. al., 2012; Llanchezhian, et. al, 2012; Elham, et. al., 2012; Zhu, et. al., 2012). In his extensive literature review of

the information security scholarship over the last decade, Honer (2013), identifies these areas as the topics most scholars are examining. Furthermore, solutions to the problems studied in the literature range from authentication and authorization protocols, the use of Private Key Infrastructure, VM isolation, network and system segmentation, encryption and auditing schemes and processes (Popovi and Hocenski, 2010; Tran, et. al., 2011; Wang, et. al., 2013). These are all important topics. However, in the applied business world, these issues are never dealt with in isolation and there is a need for broader thinking given the new agile architecture and organized threats. Studies tend to isolate factors and analyze a mixture of sub-factors which provide valuable insight but have significant practical limits when it comes to scaling and organizational decision-making. In fact, current theory, as indicated in the literature above, assumes there is a perimeter and therefore the need for dynamic scalability is not required. Previous research has indicated this is not the case and developed an alternative approach (Griffy-Brown, et. al., 2016; Gul, et. al., 2011). This approach suggests businesses should focus on cyber risk. Extending this approach and understanding risk more fully means evaluating and understanding cybercriminal behavior. Therefore, the current research through case methodology explores a systematic applied approach to identifying and evaluating new cybercrime business models using the Amit and Zott's framework for evaluating business models (Amit and Zott, 2012).

Amit and Zott (2012) in their analysis identified four major criteria. These are primarily aimed towards e-businesses so this model and these criteria were chosen because of their applicability to cybercriminal businesses:

1. **Novelty:** This refers to the renewal ability of the company. In essence, novelty refers to anything the company could be doing which represents a fresh new approach to the business previously unemployed in the industry or the market.
2. **Lock-in:** Also known as switching costs, this criterion measures the company's ability to create loyal repeat customers as well as partnerships that will not be dissolved in favor of the competition. Parties with a relationship with the company should remain with the company if ever the chance for making a choice arrives
3. **Complementarities:** This refers to how the various product lines of a single company and how complimentary are they to each other so that if a consumer is buying one, will he automatically feel the need to buy the second making his purchase more meaningful.
4. **Efficiency:** This refers to transaction efficiency and proclaims that the more the volume of transactions, the less cost incurred by the company per transaction.

This model is often referred to in citations as the NICE model and is used for evaluating new businesses for potential funding. The methodology for using this theory to evaluate cybercrime business models is explained more thoroughly in the methodology section of this study.

This research first will identify evolving cybersecurity business models and then evaluate these models based on a recognized framework. The next section will explain the methodology used to answer the research questions posed. Following this, the business models identified and their scores are explained. The final sections provide a Risk-Based approach for addressing the emergence of these dynamic models explains the broader meaning of these results for the business and scholarly communities. Based on this analysis, companies can similarly use the security framework presented as a tool for advancing further real-world solutions to these dynamic challenges.

METHODOLOGY

The data collection strategy used in this investigation is known as triangulation, involving multiple methods for collecting historical and longitudinal data (Yin, 1994; Strauss and Corbin, 2015). Multiple sources of data (e.g. participant observation, open / structured interviews, etc.) were collected through semi-structured interviews with 80 executives, an examination of reported security incidents as well as "malvertising" campaigns, websites and publically available reports from January 1, 2015 to August 1,

2016. The interviews helped this research to gain an understanding of the executive's perception, to identify the key common problems, to filter out new or unique business models, and to understand how to address these challenges through dynamic and agile solutions. Coding included highlighting issues that appeared more than 3 times in the interviews, incidents or "malvertising campaigns" as part of the construct and to identify the business models as well as develop and apply the risk-based framework. The names of organizations have been kept confidential and anonymized in the reporting of the results, particularly given the sensitivity of the information security area. The focus on identifying business models was not to develop an exhaustive list but to identify new business models that could be evaluated. The business model evaluation was conducted using Amit and Zott's NICE framework [1] who identified four major interlinked value drivers for business models. Table 1 shows the evaluation schema used for each model. A description of each of the model with examples of how they worked was included with each of the evaluation sheets which were scored independently.

TABLE 1
EVALUATION CRITERIA WITH FINAL SCORING SHEET

Business Model	**Novelty**	**Lock-in**	**Complementarities**	**Efficiency**	**Average of All Scores**
Distraction	**1 2 3 4 5**	**1 2 3 4 5**	**1 2 3 4 5**	**1 2 3 4 5**	
Targeted Espionage	**1 2 3 4 5**	**1 2 3 4 5**	**1 2 3 4 5**	**1 2 3 4 5**	
Market Manipulation	**1 2 3 4 5**	**1 2 3 4 5**	**1 2 3 4 5**	**1 2 3 4 5**	
Algorithmically Coordinated Campaigns	**1 2 3 4 5**	**1 2 3 4 5**	**1 2 3 4 5**	**1 2 3 4 5**	
Ransomware for causing Human Harm	**1 2 3 4 5**	**1 2 3 4 5**	**1 2 3 4 5**	**1 2 3 4 5**	
Mass Mobile Injection	**1 2 3 4 5**	**1 2 3 4 5**	**1 2 3 4 5**	**1 2 3 4 5**	
Source Code Injection	**1 2 3 4 5**	**1 2 3 4 5**	**1 2 3 4 5**	**1 2 3 4 5**	
Adware Injection	**1 2 3 4 5**	**1 2 3 4 5**	**1 2 3 4 5**	**1 2 3 4 5**	
Critical Asset Targeting	**1 2 3 4 5**	**1 2 3 4 5**	**1 2 3 4 5**	**1 2 3 4 5**	
BIOS-Focused	**1 2 3 4 5**	**1 2 3 4 5**	**1 2 3 4 5**	**1 2 3 4 5**	
Average Score					

Scale: 1= Very Weak; 2=Weak; 3=Viable; 4=Strong; 5=Very Strong

A simple scoring system was developed using a Likert scale to indicate from 1-5 the strength of the model in each area, with 5 representing an area of key strength in the business model and 1 indicating this criteria was weak. The models were evaluated by 70 business leaders across 11 industry verticals and the scores averaged across the model and across the evaluators. The focus was not on the meaning of an individual score or even an average score but whether or not the business models could be scored at all. Furthermore, if the average among evaluators was above "4" across all of the evaluators, this would suggest a viable and potentially strong business.

RESULTS – CYBERCRIMINAL BUSINESS MODELS AND THEIR EVALUATION

The results of the analysis enabled the identification and scoring of the ten unique cybercrime businesses models (Table 2). Of significant interest is that the majority of these models involve ransomware. This indicates ransomware is a risk factor which needs to be more carefully noted amongst business leaders. The models with the highest score had the highest ratings in efficiency, complementarity and novelty. Evaluators were unsure how to evaluate "Lock-in" given that cybercrime does not involve "choice". Therefore, the evaluators interpreted "Lock-in" based on the ability of a business model to exploit enough information for a cyber-criminal organization to repeat the same or similar exploit against the same victim. "Complementarity" was also questioned although explained and interpreted by the participants as being able to compromise multiple industry verticals or many companies within the same vertical. What these results indicate is not only the clever thought process and organizational processes involved in contemporary cybercrime but the unique revenue streams which operate often on an ability to scale and create efficiencies above and beyond just selling stolen data. Efficiency and Novelty were cited by business leaders as key elements in evaluating the models. Of great interest is the reality that a well validated framework for business model evaluation can now be applied to cybercriminal activity further indicating the sophistication of modern cybercriminal activity. This further suggests that executives and business leaders must develop even more advanced data analytics approach for dealing with cybercrime. Based on the level and sophistication of these business models validated in through these results, next steps involve analyzing and developing successful approaches for addressing these new cybercriminal dynamics.

TABLE 2
CYBERCRIME MODELS

Business Model	Description	Revenue Model	NICE score
Distraction	Ransomware as a service attacks to distract authorities prior to a major planned events (such as major theft, social disruption or neighborhood/store robbery)	Ransomware is available as an on-demand service and payment is for a specific attack at a specified time purely as a distraction for another vector attack	**4.5**
Targeted Espionage	Ransomware asking not for payment in bitcoin but for passwords or other intellectual property. This was both large scale and smaller scale targeting individuals.	Business model is downstream payoff for other exploit leveraging the information gathered or selling the information gathered. For the attacker this model simplifies process and avoids the risk of block-chain/ledger being investigated down the road.	**4.75**
Market Manipulation	Using ransomware or electronic blackmail demand a CFO divulge financial performance data ahead of the next quarterly earnings and use the information to game the equities market.	Business model requires no payment, just a zipped spreadsheet. High costs for identification and tracking but high return with the right selection material.	**4.74**
Algorithmically Coordinated Campaigns	Algorithms can be used for evasion but also campaign efficiency based around the timing of coordinated campaigns. Algorithms have also been used to set-up and tear-down	Once written the core modules can scale indefinitely and be sold as a product or service.	**4.8**

	accounts, move bitcoins round and choose random fog networks for money retrieval. Algorithms have also been used to switch-up command and control communications.		
Ransomware for causing Human Harm	Ransomware campaign that victimizes hospitals and medical centers worming through externally facing servers, deleting snapshot backups and encrypting an entire networks. This model could be applied to any critical infrastructure.	Backups are restored after ransom is paid.	**4.7**
Mass Mobile Injection	Gaining an Android or Apple footprint and using an automated set of text messages across a wide footprint installing ransomware. Could be applied to IoT (vehicles, etc).	Ransom demand to carriers or network operators.	**4.45**
Source Code Injection	Large open-source software distribution with ransomware attached.	Organization who use the software are asked to pay ransom.	**4.6**
Adware Injection	Adware/PUAs are used to auction off browser space of a compromised company. Sometimes combined with the ability worm, compromise credentials or target active directory.	Access to shell is sold to the winning bidder and used to upload whatever tools they want to target the host.	**4.74**
Critical Asset Targeting	Targeting a few critical assets and preventing restoration ahead of time. Large scale operations are most vulnerable.	Ransom of $1 less than the daily operations supported or halted by this attack.	**4.4**
BIOS-Focused	Using lower paid staff to stick in thumb drives that disable machines at the BIOS level. A link is sent after payment which restores your BIOS (but leaving a backdoor open for further exploit). Seen in hotels (delivered by cleaning staff).	Thumb drive distributers are paid per thumb drive and machine compromised. Ransom is multiplied and increased with each exploit.	**4.37**

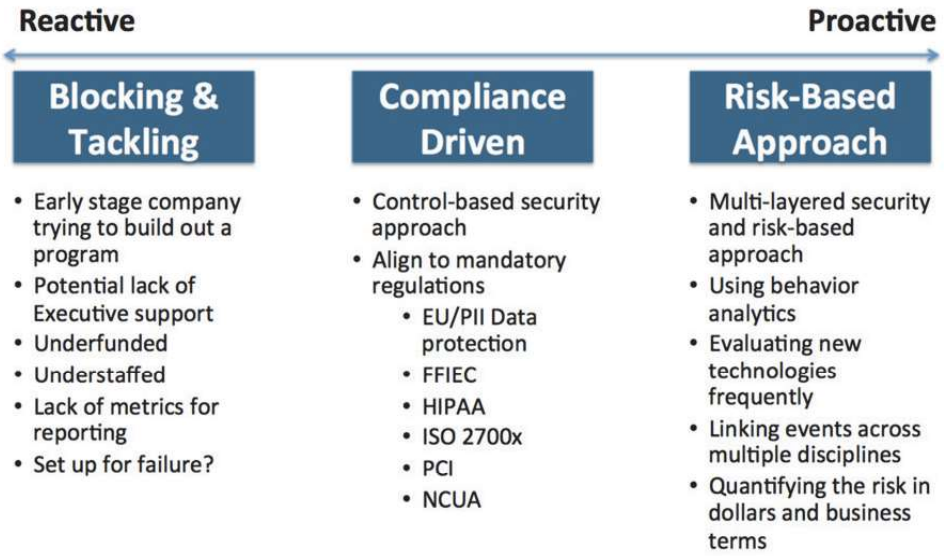
RISK-BASED APPROACH

Using a risk-based approach is something the information security industry has been socializing for over two decades. There are several risk-frameworks that have been socialized and published; however, the socialization of an Information Security Model coupled with a risk-framework has been lacking since cybercriminal activities have matured and are surpassing a legacy way of thinking.

This research connects to the Risk-Based approach by offering insight into cybercriminal behavior and how it is evolving. These considerations represent a new way of thinking that should inform the risk-

based approach in the information security maturity model. Therefore, this research fills a much-needed gap in providing a framework for continuing to evaluate new cybercriminal business models and ultimately to assign risk scores and identify potential threats as part of every business function within the organization. For addressing these dynamic and evolving issues this section will explore the application high-level security framework validated and published (Griffy-Brown, et. al, 2016) as the Information Security Maturity Model (Figure 1). In this section we will explain an applied approach that organizations can use to successfully address the challenges raised.

FIGURE 1
THE INFORMATION SECURITY MATURITY MODEL



Source: (Griffy-Brown, et. al., 2016)

This Information Security Maturity model explains that over time companies can move from a reactive state in information security to a proactive state with respect to information security (Griffy-Brown, et. al, 2016). The first column, called "Blocking and Tackling" refers to a reactive environment that is underfunded and companies are typically just reacting after criminal behavior has occurred. The next column, called "Compliance Driven" refers to a corporate environment in which a control-based approach is taken driven by audit and regulation. The final column called "the Risk Based Approach" refers to organizations which are positioned for emerging threats. They are typically using big data and behavioral analytics to understand and position themselves through a risk based approach. In this approach, businesses have a risk framework in place, widespread automation is in place and they are linking events across disciplines using dynamic controls, metrics and processes aligned with business (Griffy-Brown, et. al., 2016).

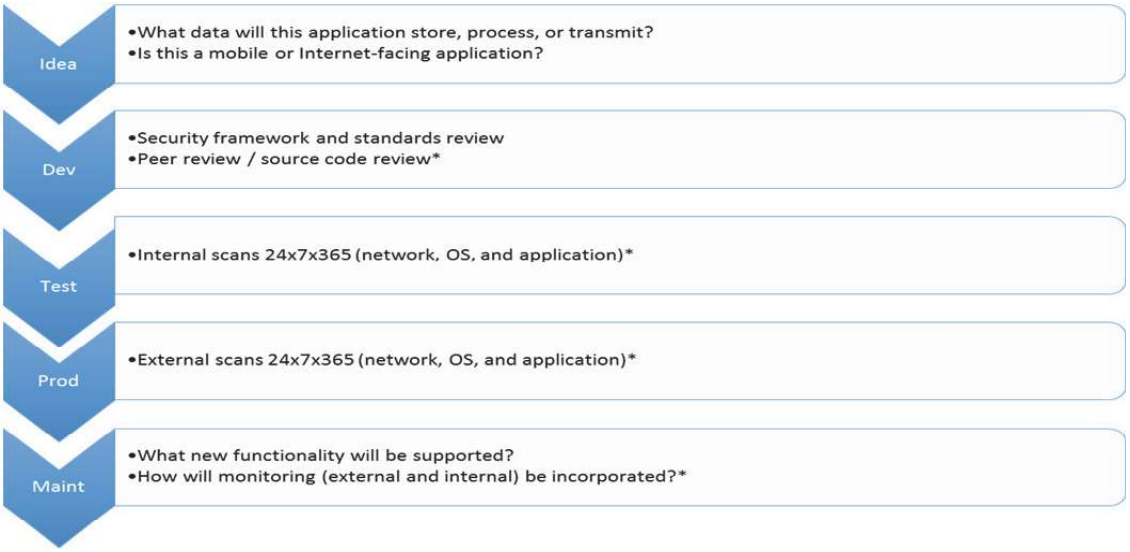
In addition, there were several approaches that consistently arose with this framework and model:

- Agile Development Striving for Continuous Integration and Continuous Delivery
- Data Mining and Big Data Analytics for Leveraging User Behavioral Analytics
- Automation
- Evaluation of Cyberliability Insurance

Organizations were still moving forward and embracing emerging technologies but these were the methods used to achieve a more risk-based approach given these dynamic environments.

More specifically, organizations were aligning information security with IT audit and the Project Management Organizations as part of agile environment development practice. To achieve this, they developed more streamlined checklists for development. Figure 2 shows an example. In this example, as you move through the development process there are exit criteria involved and these are aligned with risk. Importantly, it provides an opportunity to educate developers on security and helps developers understand how to build security into any type of development.

FIGURE 2
ALIGNING SECURITY WITH BUSINESS AND PROJECT MANAGEMENT



Source: (Griffy-Brown, et. al., 2016)

In terms of big data and behavioral analytics it is essential to have the ability to scan internal and external applications 24/7, 365 days a year. Again this is a monitoring and an educational tool. In this regard, dashboards, risk frameworks and prioritizing remediation were critical. This became part of using a risk-based approach in recognition of the fact that using the business models identified in this research, cybercriminals test corporate environments and often go undetected for more than 100 before executing some of these ransomware and other organized attacks. Table 3 provides threat landscape models. Given that IT must align to the business requirements there is a need to know what the threat vector is, create a problem statement for that vector, identify the tools that need to be implemented and show the observations, risks and gaps (Griffy-Brown, et. al., 2016). Table 3 provides a tool for doing this. This also identifies specific tools that will help with the automation and analytics. Using this checklist, items are listed out in terms of priority vectors of concern. This enables executives to tie innovation to risk and make informed decisions regarding datacenter and internet application protection in a dynamic and agile environment as businesses build out a "system of systems". This also allows executives to go after the budget they need for success recognizing the complex organized cybercriminal business models that exist today.

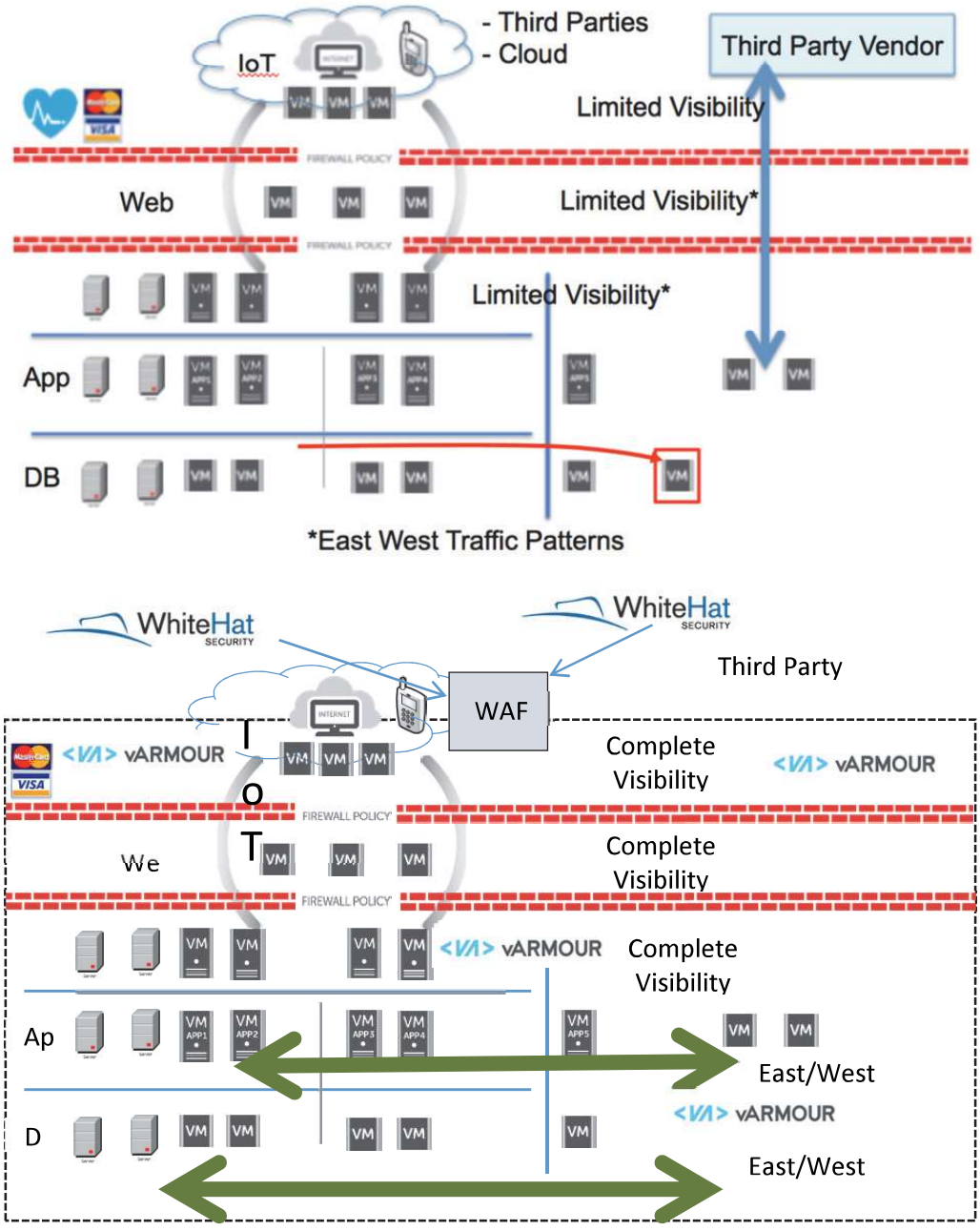
TABLE 3
THREAT LANDSCAPE MODELS FOR THE STREAMLINED BUILD-OUT CHECKLIST

Threat Vector	Problem Statement	Tools Implemented	Current Observations, Risks, and Gaps
Application Security	**Web application vulnerabilities lead to significant issues when P1s aren't resolved with current SLAs.**	• Training for developers (internal and third parties) • External and internal scans 24x7x365 (WhiteHat) • Penetration testing (3rd party quarterly tests) • Source code analysis (SCA) • Behavior analytics • WAF (Integrate with application scanning tool(s)	• **Identify where there are weaknesses within the organization** • **List and determine the level of high-risk countries or activities that may be accessing the application layer**
Network/OS/ Systems	**Virtualized environments are in scope for most regulatory compliance.** The company needs to meet agile business requirements. The company needs to detect laterally moving traffic between the data centers, zones, supporting networks, and cloud integration.	• Elasticity and agility to spin up/down environments • Network and OS scanner(s) • Management of physical and virtualized environments • File integrity monitoring • Monitoring internal (east/west) malicious traffic	• Determine how • **manage both physical and virtual regulated environments under one policy and one enterprise software solution.** .
Innovation	Automobiles Bitcoin IoT (eg. Wearables, Appliances, HVAC, Garage Doors) Virtualization	• Partner with manufacturers – insert InfoSec legal requirements into contract agreements • Application scanning 24x7x365 • Cloud integration • IoT • Physical and virtualized management	• **System of systems* will be in scope for multiple regulations – ensure that all stakeholders are involved throughout the product and project lifecycle**
Emerging Threats (Internal)	The company needs a ways to identify, monitor, and combat emerging threats once cyber criminals break the perimeter.	• Monitoring 'north / south' and 'east / west traffic'	• **Understand the rate of increase per hour, day, month, quarter, and year** • **Understand how anomalous traffic patterns are moving throughout the environment**

External Mobile Security Applications	Mobile device usage is increasing by 54% year over year. **15 mobile applications are being developed by external teams** that are out of corporate compliance and do not meet mandatory industry regulations.	• Behavior analytics software • Monitoring mobile app stores • Source code analysis (SCA) • Cyber threat research	• Ensure that all projects are onboarded using a project intake process and risks are identified earlier in the process
Mobile Security (Internal/BYOD)	The company needs to support the BYOD policy.	• Access controls (LDAP/AD) • MDM	• Need to determine how the MDM solution will scale over the next 'n' months.

Finally, this ties to the dynamic infrastructure that incorporates Agile Frameworks, extending an open API with little or no visibility into east-west traffic (Figure 3). For example, one way to accomplish this is to leverage the WhiteHat Application Program Interface (API) feed (identified in quadrant 1 of Table 3) embedded into the web application firewall which, enables scanning that can also then tie into a ticketing and tracking system. We know cybercriminals will break into systems but this can be the "first line of defense". In addition, emerging tools like vArmour provide the ability to examine east west traffic seamlessly so that information security practitioners are able to start sifting through data faster. As we are looking at data sets and building reporting off of the frameworks presented businesses can identify much quicker the different cybercriminal behaviors emerging. Figure 3 describes the architecture incorporating the new tools and processes aligned with the complicated emerging business models that cybercriminals are developing.

FIGURE 3
ARCHITECTURE, PROCESSES AND TOOLS TO ADDRESS CHALLENGES OF PROTECTING AN AGILE DATA CENTER



Importantly, as we look at data analysis, the business models identified in this study indicate that we need to think about how to combine events. Cybercriminals are not doing one attack but typically are engaged in a combined effort with these sophisticated models. As a practitioner, security doesn't want to be inundated with alerts but deal with streamlined reports such as dashboards that enable analysis and decision-making.

CONCLUSION

As a civil society and business community we are novices when it comes to understanding cyber risks and identifying potential exploits primarily because we don't think like criminals. However, as they become increasingly more sophisticated we must develop the capacity to identify and evaluate their business models in order to quickly identify an exploit while it is underway. This research demonstrates that these cybercrime business models can be evaluated as a business and are therefore extremely sophisticated. Identifying these exploits as they transpire requires understanding these models, knowledgeable use of user-behavior analytics and the risk-based approach described. It is critical that executive leadership start understanding what is going on in their organizations in terms of information security and this must be explained in business terms and aligned with business. Criminals are mobilizing and the sophistication of the breaches explored in this study validate this. As business professionals and scholars we must look at new technologies and ask how they are aligned to emerging threats. In this regard, agile development, user behavioral analytics and automaton must be tied to a big data platform. Importantly, user-behavior analytics must be architected into all future design. Finally, it is critical to audit frequently in order to understand how a business is aligned to emerging threats by ensuring companies build in dynamic controls that go beyond compliance.

This research has identified that in terms of dynamic architecture the critical security problem is that the perimeter is forever gone and criminal activity is increasingly organized and sophisticated. We have characterized and evaluated cybercriminal business models. Furthermore, the information security maturity model demonstrates how organizations are evolving and where to head to achieve better results in terms of a dynamically safe environment within this new reality in which businesses have no defensible "perimeter" because of co-mingled systems and face increasingly sophisticated threats. Finally, dynamic and agile tools and dashboards are required both in terms of decision-making processes, user behavior analytics, the development processes and ways to see across architecture to deal in a faster more effective way with cybercriminals and their coordinated efforts in an agile architecture eco-system. This research serves as a mechanism for educating executives and expanding scholarly approaches to information system security aligned with the realities of the swiftly changing cybercriminal community.

REFERENCES

Amit and Zott (2012). Creating Value through Business Model Innovation. MIT Sloan Management Review. 53: 3, http://sloanreview.mit.edu/article/creating-value-through-business-model-innovation/.

Chen, G., Miao, J., Xie, F. and Mao, H. (2013). A framework for storage security in cloud computing. Journal of Management and IT, 3:2, pp. 87-97.

Cho, G. H. and Lee, S. A. (2012) A secure service framework for handling security critical data on the public cloud. Guangzhou, China.

Chonka, A. and Abawajy, J. (2012). Detecting and mitigating HX-DoS attacks against cloud web services. 4th International CSS Symposium, Melbourne, Australia.

Chonka, A., Xiang, Y., Zhou, W. L. and Bonti, A. (2011) Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. Journal of Network and Computer Applications, 34, 4 (July 2011), 1097-1107.

Chou, Y., Levina, O. and Oetting, J. (2011). Enforcing confidentiality in a SaaS cloud environment. 19th Telecommunications Forum (TELOR) Proceedings, Belgrade, Serbia. pp.90-103.

Deshmukh, A. A., Mihovska, A. and Prasad, R. A (2012).Cloud computing security schemes:- TGOS and TMS. Information and Communication Technologies (WICT), 2012 World Congress. Trivandrum, India. Oct. 30 2012-Nov. 2 2012, pp. 203-208.

Elham, H., Lebbat, A. (2012). HX-DoS attacks against cloud web services. Melbourne, Australia.

Gul, I., Ur Rehman, A. and Islam, M. H. (2011). Cloud computing security auditing. Gyeongju, Korea, June, 21-232011. pp. 143–148.

Griffy-Brown, C., Lazarikos, D. and Chun, M. S. (2016) How Do You Secure an Environment Without a Perimeter? Using Emerging Technology Processes to Support Information Security Efforts in an Agile Data Center. Journal of Applied Business and Economics. 18:1. pp. 90-102.

Honer, P. (2013). Cloud Computing Security Requirements and Solutions: A Systematic Literature Review. Thesis. University of Twente, Faculty of Engineering and Mathematics and Computer Science. Enschede, Netherlands.

Ilanchezhian, J., Varadharassu, V., Ranjeeth, A. and Arun, K. (2012) To improve the current security model and efficiency in cloud computing using access control matrix. Proceedings of the 3rd International Conference on Computing, Communications Technology and Networking, July 21-25, 2012, Tamilnadu, India. pp.750-765.

Kumar, P.S. and Sburamanian, R. (2011). Homomorpic Storage Secruity in Cloud Computing. Infomraiotn International Interdisciplinary Journal. 14,10 (October 2011), 3465-3476.

Mandiant 2014 Threat Report (2014). Trends Beyond the Breach. https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf. Mandiant FireEye Consulting, Milipitas, CA.

Monfared, A.T. and Jaatun, M.G. (2011). Monitoring intrusions and security breaches in highly distributed cloud environments, IEEE 3rd international conference on cloud computing technology and science, *Athens*, *Greece*, pp 772–777.

Munoz, A., Gonzalez, J. and Mana, A. (2012). A Performance-Oriented Monitoring System for Security Properties in Cloud Computing Applications. Computer Journal, 55, 8 (Aug 2012), 979-994.

Nishikawa, K., Oki, K. and Matsuo A. (2012). SaaS application framework using information gateway enabling cloud service with data confidentiality. Software Engineering Conference (APSEC), 2012 19th Asia-Pacific , 4-7 Dec. 4-7, 2012. pp. 334-337. Hong Kong, China.

Popović, K. and Hocenski, Z. (2010). Cloud computing security issues and challenges. MIPRO, 2010 Proceedings of the 33rd International Convention, May 24-28, 2010, Opatija, Croatia. pp. 344-349.

Tran, D. H., Nguyen, H. L., Zha, W. and Ng, W. K. (2011). Towards security in sharing data on cloud-based social networks. 8th International Conference on Information, Communications, and Signal Processing (ICICS 2011), Singapore, Dec 2011.

Trustwave Global Security Report 2016. Trustwave Holdings, Inc. Chicago Illinois, September 2016.

Strauss & Corbin (2015). Basics of Qualitative Research: Grounded Theory Procedures and Techniques, 2nd Edition. Sage Publications. Thousand Oaks, CA.

Verizon 2016 Data Breach Investigation Report. VerizonEnterprise.com, August 2016.

Wang, S. C., Liao, W. P., Yan, K. Q., Wang, S. S. and Tsai, S. H. (2013). Security of cloud computing lightweight authentication protocol. Proceedings of the Second International Conference on Engineering and Technology Innovation 2012 (ICETI 2012), November 2-6, 2013, Kaohsiung, Taiwan. pp. 284-287.

Yin, Robert (1994). Case Study Research: Design and Methods. Sage Publications. Thousand Oaks, CA.

Zhu, J. and Wen, Q. (2012). SaaS access control research based on UCON. Digital Home (ICDH), 2012 Fourth International Conference, November 23-25, 2012. Guangzhou, China, pp.331-332.