ORACLE

Securing Information
in The New Digital Economy

Synopsis

Situation

A lucrative information black market has created a data breach epidemic. The perimeter security that most IT organizations depend on has become largely ineffective.

Why it Matters

IT organizations devote almost 70% of security resources to perimeter security controls, but while the threats are external, the vulnerabilities exploited are mostly internal.

Call to Action

Securing the new digital economy means thinking security inside out and focusing more on data and internal controls.

"If attacker sophistication outpaces defender capabilities – resulting in more destructive attacks – a wave of new regulations and corporate policies could slow innovation, with an aggregate economic impact of around $3 trillion US."

(McKinsey & World Economic Forum, 2014)

verizon

A New Hacker Economy

Over the last five years, while IT organizations were focusing on the cloud, mobile and social revolution, a black market has emerged around the acquisition and sale of personal information, intellectual property, financial data and almost any information with economic value. Each security breach teaches a lesson about the techniques and actors perpetrating these attacks and collectively these incidents serve as evidence of more dynamic market forces at work. As attackers became more persistent, IT organizations reacted to each type of breach by acquiring new security technology in an on-going escalation. In the process, the cost of information security rose and the attackers became more organized. "The attacks from ten years ago, achieved by a few freelancers, have been replaced by a layered economy of specialized hackers. The coordinated execution of these groups has fueled an emerging black market that is now estimated to be more lucrative than the illegal drug trade." (Lillian Ablon 2014)

Like most free markets, the information black market has provided an underground network that connects buyers and sellers and sets the value of information. Just as the world is producing more data than at any other point in history, these organized groups are finding new ways of stealing and monetizing information. Using information from the *Verizon 2014 Data Breach Investigations Report* and other sources, this paper provides a perspective on how companies could end the on-going escalation by re-focusing IT security investment directly on the information at risk.

The black market has expanded such that "each underground market can potentially reach up to 80,000 people and many [markets] have a global footprint." (Lillian Ablon 2014) The general availability of a wider array of tools, including hacking "as a service," point-and-click tools, and online tutorials, has allowed attackers to gain large rewards with a relatively small investment and allowed even novice users to participate.

For as little as $2 per hour, an attacker can procure a Distributed Denial of Service DDoS-for-hire-service. (Paganini 2014) If a criminal group wants to launch a denial-of-service attack, instead of creating a botnet army themselves, they could simply rent a botnet for as little as a few hundred dollars. This has fueled the epidemic with tools once reserved for the technically skilled. The black market is also a side effect of the new digital economy. As businesses expand customer experiences online and adopt new digital business models, criminals find new ways of attacking these services and exposing the systemic risks.

To help companies adapt, Oracle has teamed with Verizon to debunk the frequent sensationalism that can detract from the important facts needed to create an information security strategy. The lesson for organizations is that much of our IT security was created in a time when the black market for information was less accessible and stolen information was not easily monetized.

Oracle has teamed with Verizon to debunk the frequent sensationalism that can detract from the important facts needed to create an information security strategy.

The pricing dynamics of the black market provide global exchange rates for information. Using the pricelist (Figure 1.) as a gauge, a database administrator managing a table with a million customer credit card records would effectively be managing over $20 million dollars in black market value. Insiders who previously had no economic incentive for espionage can now reap great rewards. As an example, in 2014 it was discovered that an administrator at the Korean Credit Bureau sold the personal records of 20 million Korean citizens for approximately $390,000 US dollars. Factors like geography and vertical industry can drastically influence the price - as information gets stale, it loses value, which drives the demand for more information.

Like a "just in time" supply chain replenishing perishable goods in a grocery store, the black market economy supplies timely stolen information to meet the demand. In some cases, criminals obtaining medical records were able to file false healthcare claims, receive financial payouts and use these records to get free healthcare. The volume and relatively low price of stolen access credentials should give many companies cause for alarm because access to most corporations is now for sale on the black market. How can organizations prioritize what information to secure? The Verizon 2014 Data Breach Investigations Report (Figure 2.) shows the types of information most often stolen by insiders. The lesson is that all information is not equal – to think security inside out, IT organizations first need to classify and secure information proportional to its economic value.

Information	Price/Record
Fresh credit card data	$20-25
Stale credit card data	$2-7
Medical record	$50
Hijacked email account	$10-100
Bank account credentials	$10-1000

Figure 1. Pricelist for stolen information

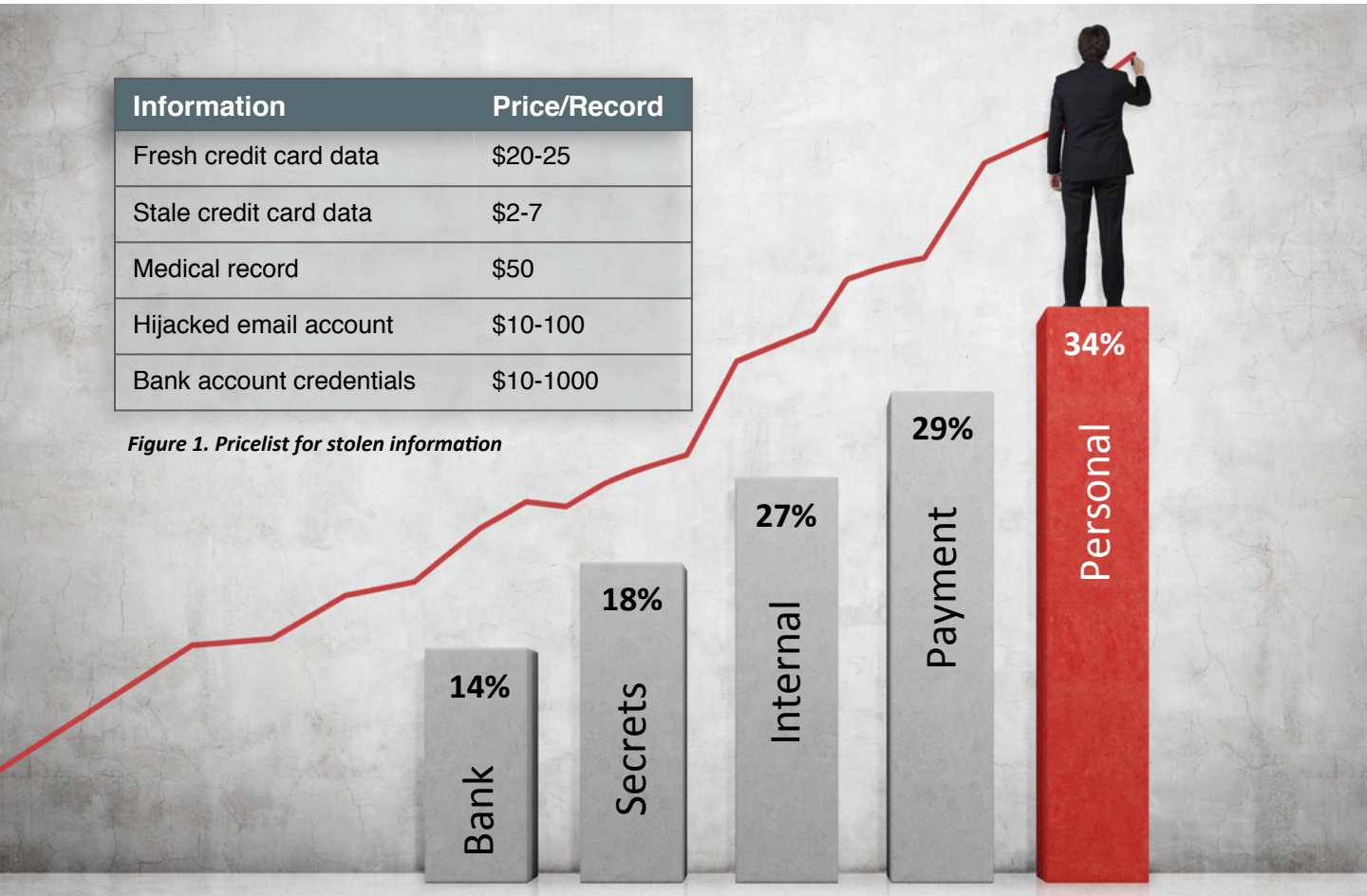

Figure 2. Variety of at risk data within insider misuse (Verizon 2014 Data Breach Investigations Report)

Threats are External, Risks are Internal

The internal security weaknesses are often exploited by hackers trying to steal data. As an example, stolen card data from point-of-sale (POS) systems has dominated the news. Most of these breaches were caused by RAM scraping malware infecting the POS systems. In most cases the malware was installed using valid user credentials that were stolen or weak enough to be cracked.

"While most organizations are focused on detecting and preventing malware, they should also focus on how criminals gained access to install malware in the first place." (Bryan Sartin, Managing Director Verizon RISK Team, 2014) To understand how criminals are breaking into organizations, we can organize breaches by category (Figure 3.) and look at the techniques used in each category.

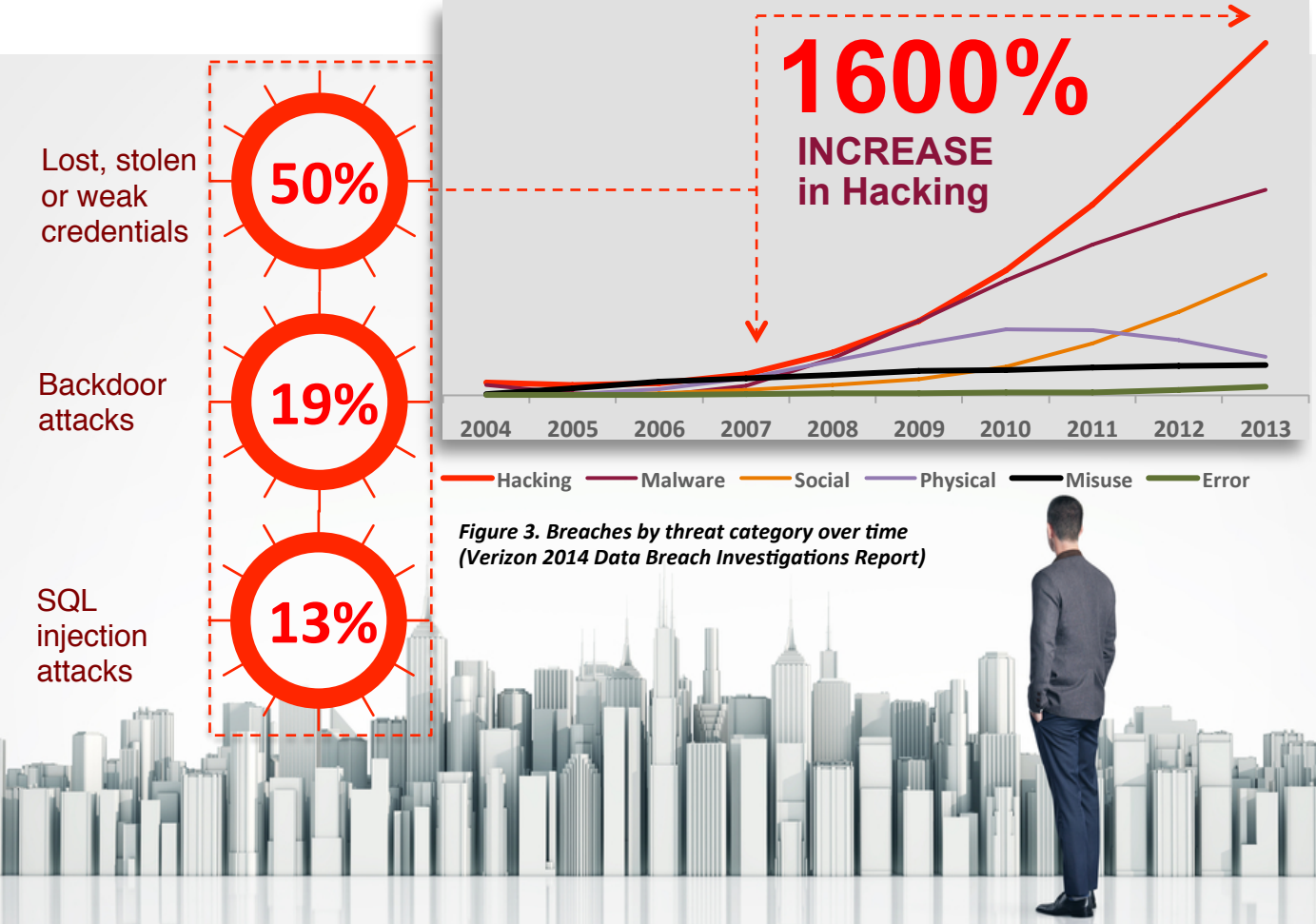

Figure 3. Breaches by threat category over time (Verizon 2014 Data Breach Investigations Report)

Hacking has continued to outpace the other means of attack by a large margin and has grown proportionally with the rise of the black market largely because the tools and knowledge are now easily accessible. From RAM scrapers to crypto malware, hacking has seen a wave of copycat innovation. These trends have also made relational databases more vulnerable than ever before. Databases are the second most frequently targeted asset by insiders. (Figure 4.)

Database Threats

According to the *Verizon 2013 Data Breach Investigations Report,* 13% of the hacking attempts were SQL injection attacks. SQL injection attacks embed SQL commands into queries in order to retrieve and modify information within the database. Most of these tips are available easily. As databases have become increasingly accessible on the network and directly from web applications, they are more vulnerable to SQL injection attacks. SQL injection attacks are challenging because they are simple to execute and difficult to prevent. An organization would have to go through their entire application code base and replace existing SQL code that is vulnerable to injection attacks. SQL injection attacks were used to dump entire tables of employee and customer records and even insert corporate spies posing as employees into HR databases. Not surprisingly, a recent study by the Ponemon Institute reported that 42% of the most serious attacks against data were SQL injection attacks. (Ponemon Institute 2014).

Despite the threats against databases, a recent study of the Independent Oracle Users Group (IOUG) found that only 38% of organizations have taken steps to prevent SQL injection attacks. Database firewalls that allow database administrators to monitor and block malicious SQL can drastically diminish these attacks. While an SQL injection attack can be damaging, much of the information today is lying around relatively unprotected in test and development environments.

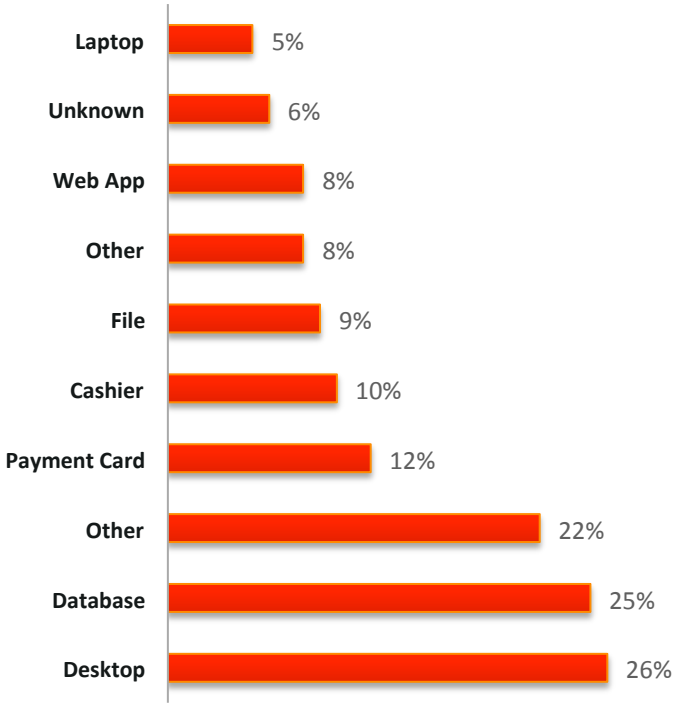

Figure 4. Top 10 assets targeted by insiders (Verizon 2014 Data Breach Investigations Report)

Developers testing applications in non-production environments typically have access to the same sensitive data used in production: salary data, revenue information, social security numbers, and credit cards. Database and application security should go hand in hand. If organizations secure applications, but leave the databases unguarded, they risk application bypass attacks. According to a study by the IOUG, 71% of organizations have no controls to prevent application bypass attacks.

Detection alone is not enough. The solution starts with good information governance and audit controls.

Building a database security strategy is the first step to security inside out. Even if the the perimeter was breached, by placing security controls around sensitive data, detecting and preventing SQL injection attacks, monitoring database activity, encrypting data at rest and in transit, redacting sensitive application data, and masking non-production databases, organizations could reduce the risk of data exfiltration. While the goal would be to eliminate breaches entirely, the first priority is to stop the exfiltration of sensitive information.

Identity Risks

What makes network intrusions so difficult to prevent completely is that attacks are occurring with legitimate user credentials, which makes criminal attacks seem like normal user access. According to the *Verizon 2013 Data Breach Investigations Report*, almost 50% of all hacking utilized lost, stolen or weak credentials. In his book *Glass Houses*, Joel Brenner, former NSA Inspector General, highlighted that criminals can purchase credentials on the black market to access nearly any institution.

According to the *Verizon 2014 Data Breach Investigations Report*, 76% of network intrusions exploited lost, stolen or weak credentials. An inside-out security strategy would have to assume that the network would be breached and instead focus on how to safeguard information while intruders were on the network. To make matters worse, the practice of sharing user credentials, while archaic, is still alive and well today. Many organizations permit administrative and privileged user password sharing with multiple people.

For the finance and accounting departments, the Sarbanes-Oxley legislation forced many companies to provide unique application user names for people accessing general ledgers and financial information.

Unfortunately, these controls did not reach far enough – access governance should also include contractor accounts, administrator accounts, application server accounts and even the accounts used on shop floors in factory settings. Shared accounts prevent monitoring of user activity, which makes detection and accountability challenging. For this reason, the Payment Card Industry Data Security Standard (PCI DSS), designed to secure payment card data, outlines the testing procedures and guidance for identifying and authenticating access to system components. Unfortunately, according to the *Verizon 2014 PCI Compliance Report*, "In 2013, 64.4% of organizations failed to restrict each account with access to cardholder data to just one user."

To complicate matters, many organizations fail to disable user access when users separate from the company. According to a CERT study of intellectual property thefts, 70% of these occurred within 30 days of employees announcing their resignation. Yet many companies can take weeks or months to remove user accounts once employees have separated from the organization. When these credentials end up on the black market, the damage is irreparable. Stolen personal information is used to propagate phishing and social engineering attacks. By simply going to Facebook and LinkedIn, criminals can derive the companies people work for, titles, who they are connected to, and even guess their work email address. With this type of information, criminals can build a strategy to infiltrate an organization using a combination of attack vectors.

Security inside-out means building security into the customer experience and employee experience. As an example, many retail and banking organizations are re-designing multi-channel customer experience with built-in fraud detection.

By simply learning the regular time a user logs on, the regular location of the user and detecting the device the user normally uses, organizations can reduce fraud from impersonation attacks. Deploying stronger controls for authentication and authorization are first steps to reducing cybercrime.

Passwords alone are not enough - adding a second factor for authentication like a mobile device can drastically increase confidence of user access.

Without solutions that automate IT security governance, users will choose weak passwords, share accounts and in general share passwords across accounts. Companies can restore control with good governance by managing privileged user access across databases, systems and applications; regularly reviewing user access to business data; remediating excessive privileges; removing dormant user accounts and managing administrative system accounts and privileged business user accounts. While the attacks increase in sophistication, the vulnerabilities that are exploited are largely internal.

Rebalancing Information Security

"You can't protect everything, and you certainly can't protect everything equally well. This is a matter of understanding the difference between diamonds and toothbrushes, as McGeorge Bundy put it. Identify the business plans and intellectual property whose loss would cause serious harm to your company. Personally identifiable and sensitive health care information … must also be protected carefully… Design your server architecture and access controls accordingly. And make sure the information is encrypted to a high standard." *(Joel Brenner, Former NSA Inspector General, "Glass Houses" 2013)*

Organizations have an imperative to act because with each new incident security professionals reactively increase budgetary spend. The net result is that organizations are spending more and losing the arms race against the black market. "If attacker sophistication outpaces defender capabilities – resulting in more destructive attacks – a wave of new regulations and corporate policies could slow innovation, with an aggregate economic impact of around $3 trillion US." (McKinsey & World Economic Forum, 2014) Taking a security inside-out approach may not only end the arms race but also give economic growth a chance.

When criminals break in, it can take only minutes for them to find the information they need and begin exfiltration. We can deter these attacks and increase the likelihood of detection by making it more costly and difficult for attackers. By focusing on the most valuable information assets, organizations can not only increase the level of difficulty, but also diminish the information supply chain. IT organizations are realizing that they can't protect everything equally well. So what assets should an organization focus on? According to the *Verizon 2014 Data Breach Investigations Report*, breaches of servers occurred more frequently than network breaches.

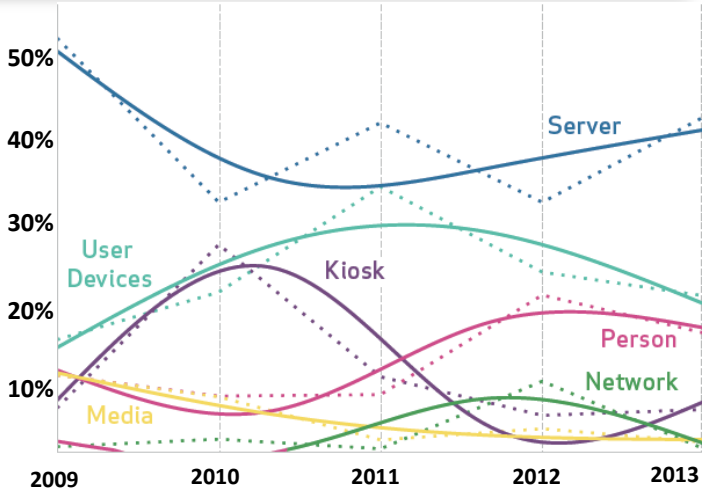

Figure 5. Percent of breaches per asset over time (Verizon 2014 Data Breach Investigations Report)

Less than 10% of breaches actually breach network assets like switches, firewalls and routers. (Figure 5.) This does not mean we should neglect network security, but rather realize that it represents only one control in a new digital economy where the perimeter is increasingly porous. Improved security controls for internal servers, applications, and databases combined with better monitoring and analysis of network traffic and server transactions would be a better approach. These internal systems have become the new perimeter and the new front line in the battle to secure corporate information.

Citations and References

- Brenner, Joel. ***Glass Houses***. Penguin Press, 2013.
- CSO Online. " **An Inside-Out Approach to Enterprise Security.**" 2013.
- 2014 IOUG Enterprise Data Security Report . **"DBA – Security Superhero**." Unisphere Research, 2014.
- Kolodgy, Charles J. ***Effective Data Leak Prevention Starts by Protecting Data at The Source***. IDC, IDC, 2011.
- Lillian Ablon, Martin C. Libicki, Andrea A. Golay. "**Markets for Cybercrime Tools and Stolen Data**." Rand Corp, 2014.
- McKinsey & World Economic Forum. "**Risk and Responsibility in a Hyperconnected World**." McKinsey & Co, 2014.
- "**Fake Target breach notification leads to phishing and complex scams**." *http://www.net-security.org*, January 13, 2014.
- Ponemon Institute . **"The SQL Injection Threat Study"** 2014.
- Reuters. **"360 Million Newly Stolen Credentials Being Sold On The Black Market."** February 26, 2014.
- SANG-HUN, CHOE. *New York Times*, January 20, 2014.
- Verizon. **"2014 PCI Compliance Report"** 2014.
- Verizon. **"2014 Verizon Data Breach Investigations Report**" Verizon, 2014.
- Verizon. **"2013 Verizon Data Breach Investigations Report**" Verizon, 2013.
- Paganini, Pierluigi. Security Affairs, **"Profiling hacking for hire services offered in the underground"** , February 18, 2014.

To Learn More:

http://www.oracle.com/security

http://www.verizonenterprise.com/solutions/security