White Paper

Will you win the war against rising data breach attacks?

Deploying AI tools, next-gen technologies and a holistic approach could substantially improve your ability to prevent, detect, thwart, and contain sophisticated stealth attacks.

Number of Records Lost and Stolen Every Day

5,505,158

Records

Figure 1.
Source: Breachlevelindex.com[1]

Overview

Data breaches are on the rise, and hackers are increasingly more aggressive, with hacking incidents almost doubling since 2013[2,3] (see Figure 2). "2016 was a record year for data breaches"[19] with more than 4,000 incidents logged and over 4.1 billion customer records exposed, a 40% increase (in incidents) from the year before. Across numerous industries, from entertainment to banking, insurance to retailers, shipping to logistics/transportation, Fortune 500 and smaller companies have suffered massive financial losses and reputational damage[4]. Anthem (80M records)[3,14], J.P. Morgan Chase Bank (83M), and Sony (1TB+) are just a handful of companies who have become recent victims of super-sized (mega) data breaches with tens of millions of sensitive client records stolen. Data stolen ranges the whole gamut, from Social Security[19], employment records, dates of birth, to financial history and investment records.

Hackers Do Not Discriminate

Large or small[11, 4], publicly traded or not, financially successful or not, hackers are motivated to cause havoc by monetizing stolen records and/or holding companies' digital assets for ransom. Blue Toad, a small digital publishing firm that hosts around 5,000 worldwide publications joined Target and other victims as hackers stole more than a million identification numbers for Apple mobile devices from the firm. Targets includes both unstructured (email, communications, file shares) and structured data (CRM systems, core database systems, source code repositories).

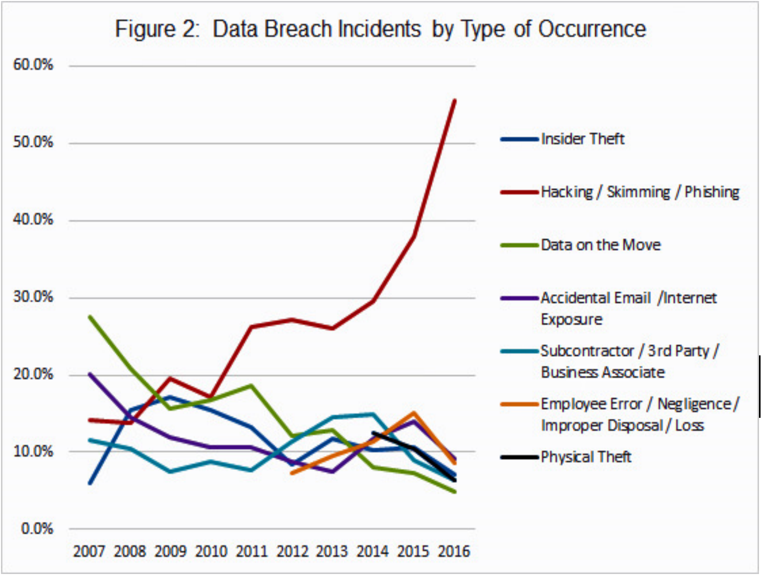


Figure 2: Data Breach Incidents by Type of Occurrence

Sophisticated Hackers and Increased Digitalization Increase Companies' Data Breach Risks

As companies and industries shift to digital business they increasingly amass a wealth of valuable digital assets along with electronic client data making them a prime target for hackers. Recent data breaches have not only resulted in super-sized numbers of stolen records but have also caused substantial negative publicity, wasted executives' time on PR and putting out fires and financial damages. Target, Home Depot and Anthem each sustained $18.5M, $19.5M and a whopping $115M in data breach settlements[7,8,14]. It has also been estimated that ongoing costs for Anthem will exceed $100M for things like credit watch monitoring for their compromised customers. Hackers are increasingly sophisticated and have been able to penetrate perimeter security undetected for several months. When customers hear that their personal information has been exposed for months, and the exposure has been undetected, the reputational damage is much higher.

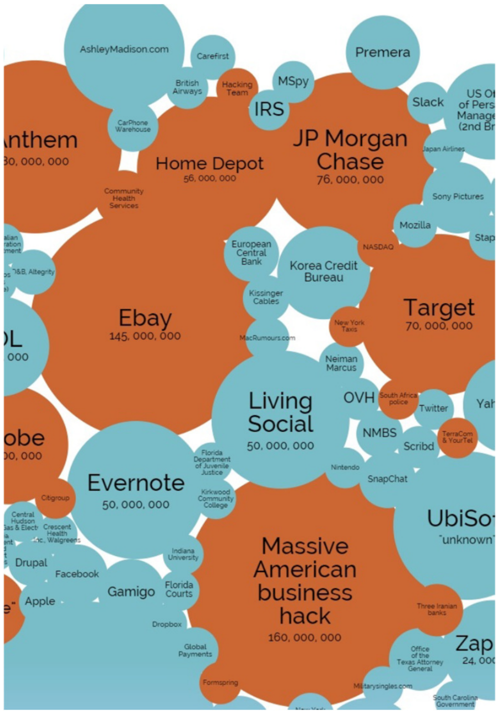
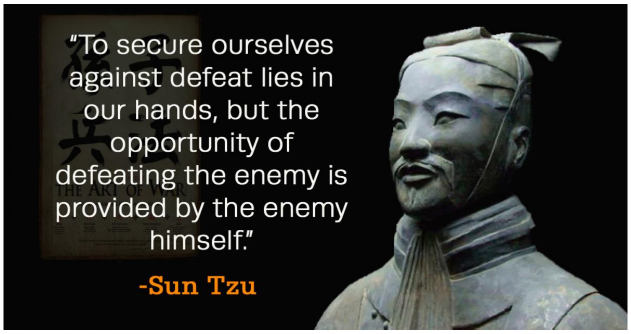


Figure 3: Super-sized data breaches have occurred across industry in recent years. From banks to retailers, healthcare organizations and insurance carriers, tens of millions of records containing PII (social security, date and place of birth, etc.), PHI and other sensitive data have been stolen. As hacking threats increase at break-neck speed, **it is not a matter of if but when a company** will be next on the victim list.[3]

Defense in Depth

Preventing against all attack vectors may be challenging, if not cost prohibitive or impossible. Persistent and highly motivated hackers may be able to compromise your network, and win the battle[12]. However, if you can stop them from removing your data, you could win the war[10]. A multi-layered defense posture may not eliminate the possibility of you losing the occasional battle, but it would better protect your crown jewels.


"To secure ourselves against defeat lies in our hands, but the opportunity of defeating the enemy is provided by the enemy himself."

-Sun Tzu

Traditional and standard security solutions seeking to defend perimeters with the use of static hardware appliances are no longer sufficient. While network prevention may be necessary as the first line of defense, companies need to shift to new innovative ways and embrace a multi-layered and robust data exfiltration prevention program that ensures not only protection of the perimeter, but also robust protection of its most valuable data assets, the crown jewels - structured and unstructured sensitive data - and have mechanisms in place to detect, and stop an attack. It's only by protecting your crown jewels will you win the war.

You can win the war

Fortunately, new technology enabled by artificial intelligence (AI) based tools coupled with real-time alert mechanisms allows companies to detect and respond faster. A multi-layered defense posture, including pre-infection measures to keep threats out, real-time monitoring capabilities to detect intrusions, and a predefined incident response plan (IRP) to find and contain active infections and illegal data transfer, will not only improve a company's ability to prevent and defend against aggressive stealth attacks but also thwart and contain any attack in progress.

A Better Practice Framework - "Defend, Detect and Contain" Strategy

A multi-prong defense strategy encompasses multi-layered systems that include traditional security solutions but also technological capabilities to protect both structured and unstructured data. The strategy must also include strong governance, pre-defined and standardized procedures to handle emergency situations and attacks to avoid costly operational errors resulting from a "fog of war" that arises during a state of chaos. Additionally, people factors like employee awareness and training, and culture change must be considered. For smaller companies, a less cost-prohibitive cloud-based solution that packages some of these capabilities as services may be appropriate (see inset – About Cloud Security Solutions)

Existing perimeter defense systems need to be able to respond to Zero Day attacks in a timely manner, without a large effort in patching hardware appliances. Threats can go global in minutes. Signatures, where used, must be continuously and automatically updated to ensure the protection against the latest threats. Additional heuristics are needed to alert to new types of traffic flows through the perimeter infrastructure, which may signal an attack.

About Cloud Security Solutions

Next-Gen Security Technologies Increase Effectiveness and Efficiencies while Reduces Costs[6]

Cloud next-gen technologies allow companies to:

- Leverage advanced AI, tools and technologies as a service
- Reduce expensive hardware and software cost
- Reduce IT, security and support headcount
- Improve productivity
- Provide a consistent user security experience on-net and off-net
- Enable and improved security for remote/mobile users
- Scale quickly and cheaply without jeopardizing availability and latency

Data Loss Prevention (DLP) is necessary to trap sensitive data leaving the organization, as any data exfiltration attack will need to extract the data from your organization. DLP forms another layer of defense, as attackers may have intruded your environment, but may not yet have extracted that data.

It is also imperative that all SSL traffic is inspected. Over half the Internet is now encrypted via HTTPS, so it is no longer sufficient to just ignore encrypted traffic. Attacks occur from encrypted sites, and data may be extracted over SSL secured transmissions.

The "perimeter" must also be extended to include mobile devices, as much of the work users do is now done on mobile devices, so it is not sufficient to protect them when they reconnect to the corporate network. Mobile devices must be protected both "on net" and "off net".

Within the perimeter, additional layers of protection are needed closer to the "crown jewels" of customer data. For unstructured data (network shares and SharePoint), tooling should include the ability to detect unusual traffic patterns from internal users. These patterns may indicate data siphoning by a disgruntled team member, or an unwitting ransomware attack in progress. For structured data (databases), new application servers, or new traffic patterns from existing application servers may indicate a SQL Injection attack designed to steal data. Both these defense mechanisms must be able to alert security personnel in real time, as "time to respond" is critical in any attack.

It is also essential to plan for when you lose a battle. Backups are essential to provide "point in time" protection should you be compromised, and data is corrupted by an attacker.

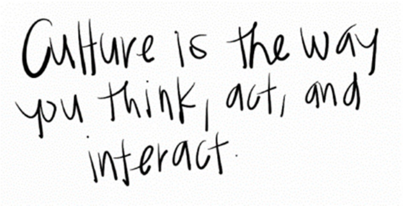
Rapid Response

The first few minutes after detection may be the most critical time to contain the infection, and it is important to have a pre-defined plan that caters to the type of incident. The response to a Ransomware attack is likely to be different to finding that all your client data has been stolen, but it is imperative that a pre-defined plan[13], with call trees, contact points and procedures is followed in those first few critical minutes.

People

People considerations need to be factored into the strategy. Sophisticated technologies, security and technical expertise and well-defined procedures alone are insufficient for an effective strategy. Proper training programs and addressing your organization's attitude towards security is necessary to ensure your multi-layered strategy will be effective.

Training employees about data privacy and security is criticall[17]. 56% (up from 38% in 2015) of attacks use a method called phishing[15,19] where employees are tricked into clicking an email link to give hackers access to corporate systems and data. Take University of California Davis Health's incident in May of this year as an example. An employee who responded to a phishing email allowed a hacker to obtain data that compromised 15,000 patients' personal health information (PHI). Had the employee been educated to identify characteristics of a phishing email, this attack could conceivably have been avoided.



Cultivation of the right (employee) attitudes and behaviors is just as important. Employee training, combined with the reinforcement of the right behaviors is key to improve a company's overall security posture. The responsibility for data security cannot be contained to just the CISO or security team. Like good citizens of a society, it is everyone's responsibility to recognize and report illegal or suspicious activity, and a company's employees and contractors can and should be able to do the same. Training is necessary to help employees and workers identify suspicious activities or behaviors. This includes executives, who are often primary targets of spear-fishing[14] attacks.

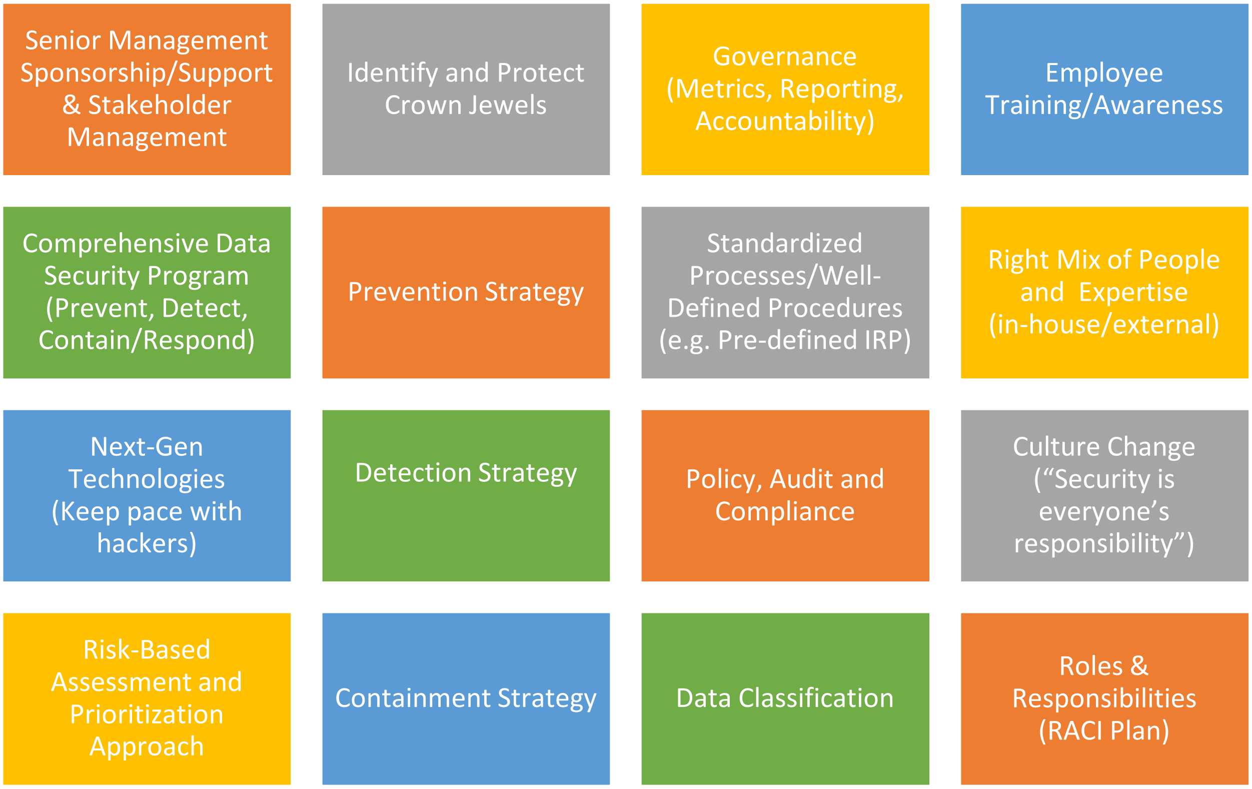
Conclusion

Each company's risk[12] for an attack is different, as is the degree of losses at stake. To determine a holistic solution that best fits your company's risk profile and needs, consider implementing an approach and roadmap that factors in the elements[9,12] depicted in the framework (Figure 4) below.

Keys to Success

Pillars of a strong and robust data protection program are multi-faceted: from leadership and strong sponsorship to deploying next-gen technologies and having the right people, tools, policies, governance and subject matter expertise, many elements must be considered for your data security program strategy to be effective.

The undertaking to improve a company's data protection capability is complex, the effort for which should not be underestimated and must be approached holistically as a multi-phased program, and not as a one-off project. The consequences of not doing so would result in wasted investment, productivity loss, and a slap-dash data security program that does little to prevent, let alone detect and stop a large-scale infection.



Senior Management Sponsorship/Support & Stakeholder Management

Identify and Protect Crown Jewels

Governance (Metrics, Reporting, Accountability)

Employee Training/Awareness

Comprehensive Data Security Program (Prevent, Detect, Contain/Respond)

Prevention Strategy

Standardized Processes/Well-Defined Procedures (e.g. Pre-defined IRP)

Right Mix of People and Expertise (in-house/external)

Next-Gen Technologies (Keep pace with hackers)

Detection Strategy

Policy, Audit and Compliance

Culture Change ("Security is everyone's responsibility")

Risk-Based Assessment and Prioritization Approach

Containment Strategy

Data Classification

Roles & Responsibilities (RACI Plan)

Figure 4 - Data Exfiltration Framework[20]

TO LEARN MORE ABOUT THIS FRAMEWORK AND THE LATEST GENERATION OF DATA SECURITY TECHNOLOGY, CONTACT US FOR A FREE CONSULTATION.

Data Exfiltration Capability Self-Assessment

Is your organization sufficiently prepared to prevent, defend, detect and contain stealth attacks?

Here's one way to find out. How many of these questions can you respond to with confidence if asked by your board of directors or senior management team[4]?

- What are our biggest data security risks?
- What is our strategy to mitigate those risks?
- How frequently do we assess our risks?
- Are our risks assessed continuously?
- What are our crown jewels?
- Where do they reside/are they stored?
- Who are our critical data owners? What level of engagement do we have with them?
- What mechanisms do we use to properly classify data?
- On a scale of 1-10, how well protected should our crown jewels be? On a scale of 1-10, how well protected are they currently?
- What is the gap between where we should be and where we are today?
- How are those gaps being addressed?
- Are those gaps being addressed using the best defense, detection and containment capabilities and technology available?
- Have we tested how well protected we are recently?
- Can we detect stealth attacks?
- How frequently should we be testing our protection?
- How do we know our systems are infected?
- How quickly can we detect an infection?
- What is our incident response plan?
- How quickly can we contain an attack?
- What is our mitigation plan?
- What is our backup plan?
- Do we have the expertise in-house to do all that is needed to secure our data at the levels needed?

About Hararei, Inc.

Hararei is a strategic IT and infrastructure boutique consultancy firm and channel partner for leading-edge cloud, security, network and data management solutions.

This Publication

This publication is written in collaboration with Arete Advisors LLC, ("Areté"), a strategic alliance. Areté (pronounced ah-ree-tay) is a boutique management consultancy that specializes in transformational and organizational change management, governance, process/continuous improvement, LEAN, and program management**.** Visit www.areteadvisorsltd.com.

Disclaimer

This publication does not constitute professional advice and you should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, Hararei, Inc. does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

Product Channel Partner

Hararei, Inc. is a proud channel partner and value-add reseller of leading cyber-security products. Contact us to schedule a free demonstration of these and other products.

zscaler®
Secure. Everywhere.

Zscaler enables secure, policy-based access to the Internet. Block attacks are in real time with network security that is always inline, cost-effective and easy to deploy. Protect your employees from malware (including Ransomware), viruses and other internet threats, blocking attacks in real time. Zscaler security services scan and filter every byte of your network traffic, *including SSL-encrypted sessions*, as it passes to and from the internet.

VARONIS
IS YOUR DATA
AT RISK?

Varonis is the only company that can monitor, manage and protect human–generated data in critical file systems, email, intranets, and file shares, while at the same time increasing employee productivity and reducing costs, and only Varonis have proven that they can do it at scale

DB NETWORKS

DB Networks next generation technology is based on database infrastructure sensors, deep protocol extraction, machine learning, and behavioral analysis. The technology is foundational to achieving the ultimate vision of autonomous cybersecurity.

druva

Druva is a Cloud Native data protection technology that can protect your data whether it is on-premise, or in the Cloud. The technology is data protection technology that was "born in the cloud" to address the unique challenges of protecting your sensitive data wherever it may reside.

Resources

1. “Data Breach Statistics”, Breach Level Index. June 2017.
2. “Data breaches increase 40 percent in 2016”, Identity Theft Resource Center. January 2017.
3. “World’s biggest data breaches”, Information is Beautiful. April 2017.
4. “2015 Information Security Breaches Survey”, PWC, InfoSecurity Europe, and HM Government. 2015.
5. “Data Exfiltration Demystified”, Ben Cody, Intel Security. 2015.
6. “How cloud computing helps cut costs, boost profits”, Thor Olavsrud, www.cio.com. March 2013.
7. “2016 Cost of Data Breach Study: Global Analysis”, Ponemon Institute LLC. June 2016.
8. “Top Breaches”, Breach Level Index. June 2016.
9. “Top ten tips to prevent data exfiltration”, SecurityWing. January 2016.
10. “Preventing and Responding to Data Breaches”, Jackson Walker LLP. n.d.
11. “Don’t become the next Sony: How HR can win the war on data”, Pat Didomenico, Business Management. January 2015.
12. “Building a new data breach policy”, Jac Brittain, LPM (Loss Prevention Media) Insider. June 2017.
13. “Data breach response”, Federal Trade Commission. September 2016.
14. “2016 Data Breach Investigations Report”, Verizon. 2016.
15. “Phishing Data – Attack Statistics”, Darren Dalasta, Infosec Institute. 2017.
16. “The Latest in Phishing: March 2016”, Mike Bailey, WombatBlog. March 2016.
17. “Phishing attacks prevention”, Nate Lord, Digital Guardian. June 2017.
18. “Attackers target both large and small businesses”, Symantec. 2016.
19. “2016 a record year for data breaches”, Olga Kharif, Bloomberg.com. January 2017.
20. Arete Advisors Data Exfiltration Framework. Source: https://www.areteadvisorsltd.com/ourmethodologies. 2017.

hararei

Your Edge Solutions Provider

Specialists in innovative cloud, cybersecurity, and infrastructure solutions
that lower costs, increase agility, improve productivity, and reduce risks.

Website: www.hararei.com
Phone: +1 (702) 608-8283
Email: contact@hararei.com

For more information, contact:

Mark Snodgrass
Managing Director
Email: Mark.Snodgrass@hararei.com

areté Achieve more with *less*

Boutique management consultancy – Helping clients address
people, process, governance, program management and risk management challenges.

Website: www.areteadvisorsltd.com
Phone: +1 (862) 295-1488
Email: contact@areteadvisorsltd.com