WISEGATE ANSWERS

DRILL-DOWN REPORT

Malware & Data Breaches:

Combatting the Biggest Threat

CONTENTS

Summary

Malware & Data Breaches
TOP TAKEAWAYS

» **CISOs consider malware and sensitive data breaches to be their top risk.** It is not malware *per se* that is the greatest threat, but specifically that malware that can lead to a breach of sensitive information.

» **Malware cannot be definitively excluded.** Taking a pragmatic view, CISOs are beginning to concentrate on detecting what they cannot prevent.

» **BYOD and cloud adoption is eliminating defendable perimeters.** Since it is no longer possible to keep data within a controlled environment, CISOs are choosing to protect the data above the device.

Wisegate recently conducted a member-driven research initiative designed to assess the current state of security risks and controls in business today. *Assessing IT Security Risks* addresses many of the top takeaways from that survey. This current document is the second in a new series of reports designed to look more closely at four specific issues highlighted by that survey.

- Metrics and reporting
- **Malware and data breaches**
- Data-centric security
- Automation and orchestration

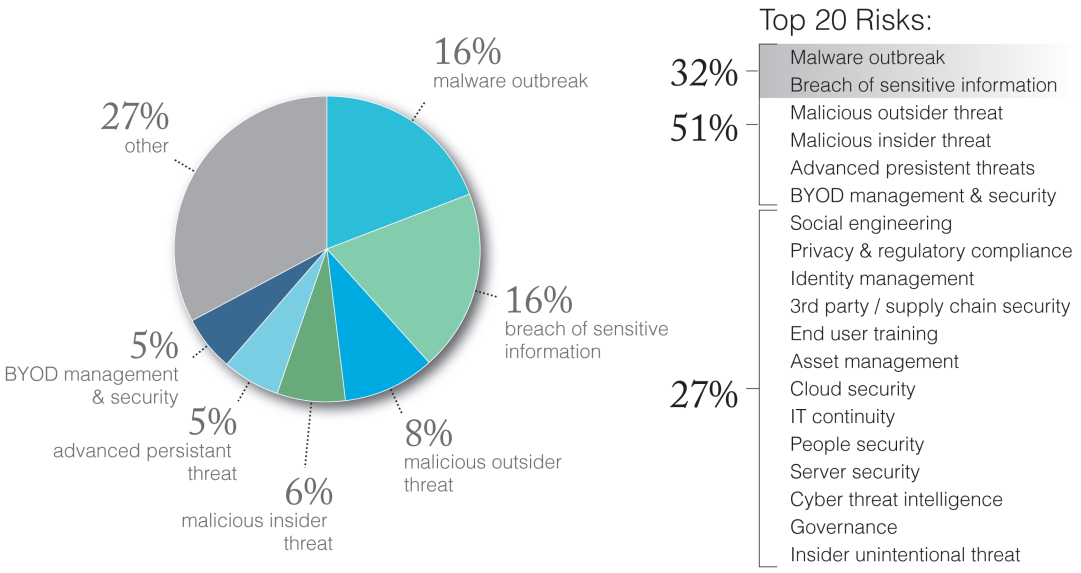
Malware and Data Breaches

One of the top takeaways from the Wisegate survey is the extent to which malware and sensitive data breaches dominate CISO concerns. The survey asked participants to name their top three risks. It was a freeform question in which participants could specify any risk at all. Malware and breaches of sensitive information were both specified by 16% of the respondents. Third and fourth were malicious outsider threat and malicious insider threat at 8% and 6% respectively, with a long following tail (see Figure 1). In all, almost 80 different 'risks' were specified.

In reality, says Bill Burns, lead author of the survey, *malware* is a threat, not a risk. The risk is the *breach*—but respondents made no distinction between risks and threats and treated the two as one. In this instance, the close correlation in concern over malware and sensitive

data breaches implies that it is not malware *per se* that causes concern to CISOs, but specifically the malware that can or does lead to a breach of sensitive information.

Figure 1. Survey Question: What are your top three security risks?



Source: Wisegate June 2014

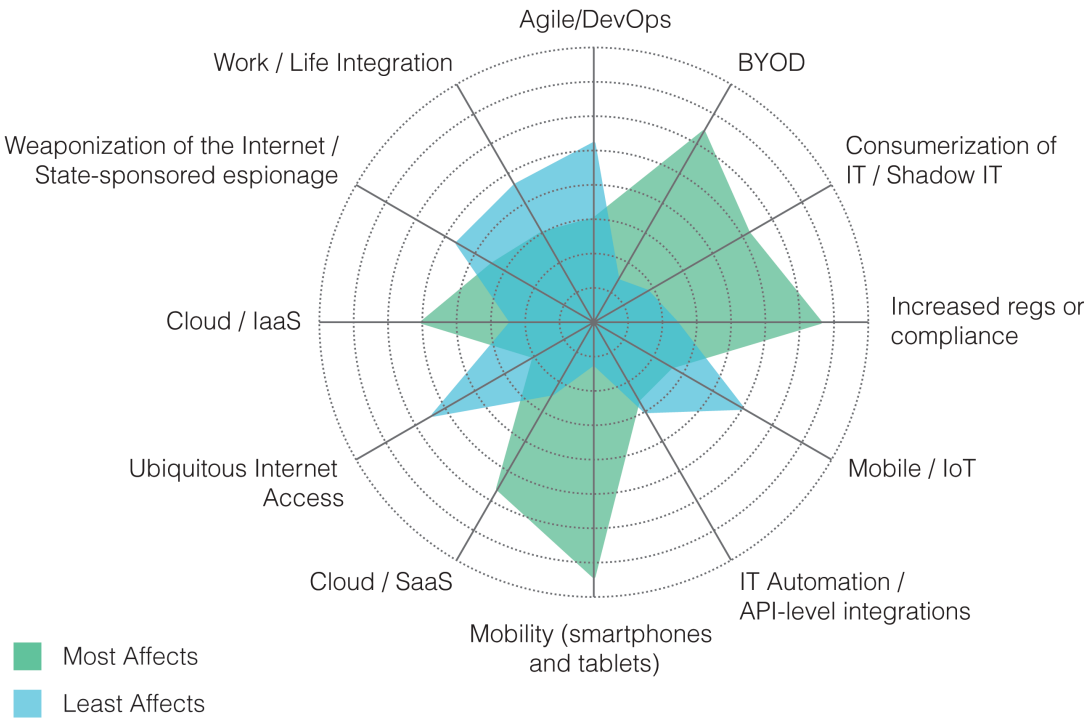
"A data breach and the loss of sensitive information is not the only risk associated with malware," explains Burns. *"The malware could be destructive (think of Stuxnet and Wiper), or for competitive or domestic surveillance purposes. It could be targeted to steal personal data for blackmail (think celebrity photos or webcam controllers); or it could be economic, stealing bank details or autodialing premium rate phone numbers."*

None of this seems as high on CISOs' list of concerns as the loss of sensitive information. That sensitive information is likely to be customer/client PII or PIH, and/or company IP. It is the loss of this sort of information that will be the most painful to business, in the costs of remediation, forensic examination, breach notification, loss of brand reputation and potential legal costs. Security is increasingly led by risk management principles, which require the greatest effort in the areas of greatest risk to the company. Large-scale loss of sensitive information is clearly considered to be a major threat.

Current Trends

The survey also asked participants to specify the trends that most affect their security program (see Figure 2). The response shows clear concern over BYOD and cloud (a third, concern over compliance regulations, is a separate and almost self-contained issue).

Figure 2. Survey Question: Which of these trends most / least affect your security program?



Source: Wisegate, June 2014

When we combine these two sets of responses, it is clear that a combination of malware leading to a breach of sensitive information, BYOD and the cloud are a major concern to CISOs.

Current Trends and the Malware Threat

Burns believes that the malware threat and its associated data breach risk is likely to get worse over the coming years specifically because of these trends:

- the continuing evolution of BYOD practices
- increasing adoption of cloud technology, both public and private

Malware is already unstoppable, even in a traditional IT environment that only has to defend a known and controlled perimeter with a relatively small attack surface. The combination of cloud and BYOD removes the defensible perimeter and increases the attack surface dramatically.

Defending the BYOD attack surface

"What I see," explains Burns, *"is a world where employers will actually require people to bring and use their own devices. Most companies already provide staff with equipment, and many currently tolerate BYOD. The trend will continue until eventually companies will say, 'Well, if you're going to have a phone and a computer in your personal life, why don't we just keep using those?' Why, in fact, would a company wish to buy stuff that its employee already has and is already using?"*

But this leads to a tension between company and personal information held on the same device. *"The company will need to protect its own data, but the personal data will be in conflict with any device monitoring that the company does,"* says Burns. In short, there is potential for a Big Brother inspired kickback from the employee.

This is already happening. At a Wisegate roundtable discussion on BYOD practices, one member from a major O&G services company commented,

> *"We've always had the ability to completely wipe the BYO device [via ActiveSync] built into the corporate email policy. We had no complaints. But when we moved to an MDM approach and explained to the users that corporate and personal data would be kept separate, and that we would know the difference, we suddenly got resistance. There were many comments about a Big Brother approach. We found the users don't want the company they work for to know what is on their device. Some have chosen not to register with the MDM, either insisting on a company device or not having the access capability at all."*[1]

An MDM product that keeps corporate and personal data in separate containers on the mobile device is not enough on its own. *"The savvy security team,"* suggests Burns, *"will earn the user's trust by demonstrating that the company can only monitor the corporate data, and not only doesn't, but cannot monitor anything else. As soon as Security can establish that level of trust with the employee, then two things happen. Firstly, I get greater assurance that the user is following my security guidelines and is installing the right protective measures on personal devices to protect the company and company data. Secondly, it allows the employee to say, 'Gosh, this security stuff is really complicated—but I don't need to worry because I can leverage the company team as my own personal security team.'"*

[1] BYOD Series, Part 2 - Data, Tools, Management and Rules

In short, says Burns, the employee loads the correct protective controls to protect the company in the knowledge that all personal data is private from the company and secure from the criminals. It becomes a partnership based on mutual trust, where the employee protects the company, and the company security team protects the employee and the employee's private and family data.

"This," suggests Burns, *"is doable through a combination of both product and corporate culture."* On the product front it is an extension of the container approach already used by MDMs, but specifically designed to prevent any corporate access to personal data at all, and to engender that level of trust in the user. This is one approach to minimizing the malware threat on BYO devices.

The Cloud and BYOD

An alternative BYOD policy, suggests Burns, is to say, *"I cannot possibly defend all possible endpoint platforms, so I won't even try. I'll push everything into the cloud accessible by browser only. The browser will give a view of the data, but not allow any copying to or processing on the local device."* This, he suggests, is a good security posture. But it is not easily achievable in practice, and has numerous pitfalls along the route.

One problem is actually implementing such an approach. *"There is a tension,"* suggests Burns, *"between the 'view only' approach and the increasing power of the mobile device."* It is a tension that has not been solved—the reality is that some processing is best done locally. *"Maybe it's not a binary decision,"* he continued. *"Depending on the corporate culture, either is a satisfactory experience. Perhaps the decision determining whether the data stays in the cloud or can be processed locally should depend on the sensitivity of the data. Maybe it's a data classification or data sensitivity decision point."*

Using the cloud to defend against malware-inspired sensitive breaches is a strong argument. It is harder to infect the cloud than it is to infect an individual endpoint. But there is also a scale issue. *"If I, as an attacker,"* explains Burns, *"manage to infect the cloud, I potentially get to impact many more customers and much larger datasets."*

The weakness in cloud security is less the cloud itself and more how the cloud is used. This is an aspect of something that Burns considers to be one of the biggest challenges to IT security: the difference between something working correctly and something working correctly and securely. This affects everything from malware prevention to proprietary apps, open source software and websites.

A good example of this problem is the fate of Code Spaces. Code Spaces used AWS cloud services to store customers' code. Everything worked correctly. But when Code Spaces was compromised, everything belonging to all Code Spaces customers was affected—and in the event actually lost. Code Spaces itself went out of business.

The problem wasn't the cloud nor was it AWS—it was Code Spaces poor use of AWS. It did not use Amazon's 2FA option; it had no DR plan; it stored its back-up effectively in the same room (that is, in the same AWS account); and it discussed its response over a compromised channel when it should have been out of band. Because of the latter, the hacker was always one step ahead, and decided to delete content and get out. AWS (that is, the cloud proper) was never itself compromised.

"Working correctly is different to working securely," explains Burns. *"In the physical world we get visual clues. You can go into a brick and mortar bank and see at a glance if it doesn't look secure. But if a web page works correctly, there is nothing to show whether it is also secure."* This *"if it works OK it must be OK"* thinking is why so many users get infected by malware through poisoned websites and malvertising—and indeed cleverly crafted phishing emails with weaponized attachments.

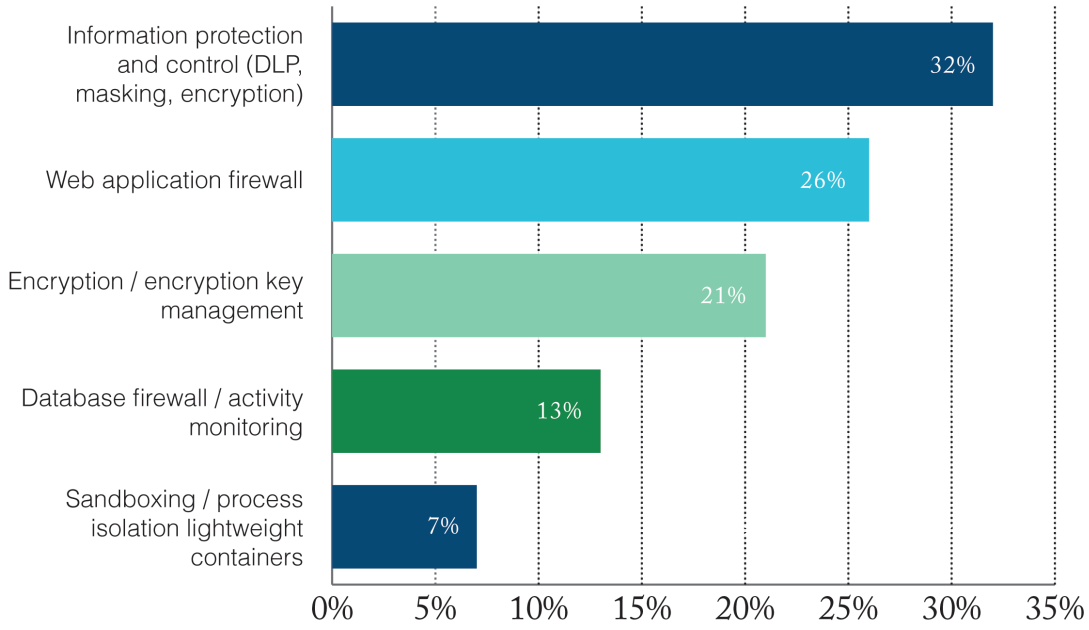
Trends and the IT Infrastructure

What is clear from current trends is that IT infrastructure is in the midst of the biggest structural change since user computing migrated from the computer room to the desktop. Now it is leaving the building altogether—moving to users' mobile devices with no fixed location, and into the nebulous cloud. What this means for security is that there is neither an infrastructure perimeter to defend nor much knowledge of where company information actually resides. Traditional security controls that defend the trusted network perimeter no longer apply—which means that new security controls are necessary.

The survey asked what infrastructure security controls would be prioritized over the new few years (see Figure 3).

It is clear from the responses that there is less emphasis on protecting devices and greater emphasis on protecting applications and the data itself. Firewalls are now application firewalls rather than trusted network firewalls—and encryption figures in both the top and third response. Data leak prevention as the favored control demonstrates that malware prevention has been replaced by malware detection as a priority. Encryption is designed to protect the data itself, so that even if there is a breach of sensitive information, that information remains hidden from any attacker.

Figure 3. Survey Question: Which of these Infrastructure controls will be a top priority to you in the next 3-5 years (multiple selections allowed).



Source: Wisegate, June 2014

This is a pragmatic view of security. Faced with the impossibility of defending against malware attacks in the new cloud/BYOD paradigm, security is engaged in a massive shift from protecting devices to protecting data. This new paradigm—date centric security—will be discussed in greater detail in the third report of this series. If the data itself is safe, it doesn't' matter if the malware results in a breach.

Membership
HAS ITS ADVANTAGES

Wisegate is a new kind of advisory service built on the collective expertise of IT leaders. We provide unbiased feedback, experienced insight, and actionable information to our members through an anytime, always-on website, concierge service and mobile app.

Wisegate upholds a high bar for its members because it is through these members that we gather our curated information in the forms of polls, Q&A, product reviews, document sharing, roundtables and working groups. 100% of Wisegate members are senior level, and 89% of them have more than 16+ years experience in IT. There are no vendors, analysts, or inexperienced IT professionals in the Wisegate network.

Would you like to join us? Go to wisegateit.com/request-invite/ to learn more and to submit your request for membership.

PHONE 512.763.0555

EMAIL info@wisegateit.com

www.wisegateit.com