BIOS
desktop to datacenter

WHAT EVERY CEO, CIO AND CFO NEEDS TO KNOW ABOUT CYBER SECURITY.

A guide for IT security from BIOS

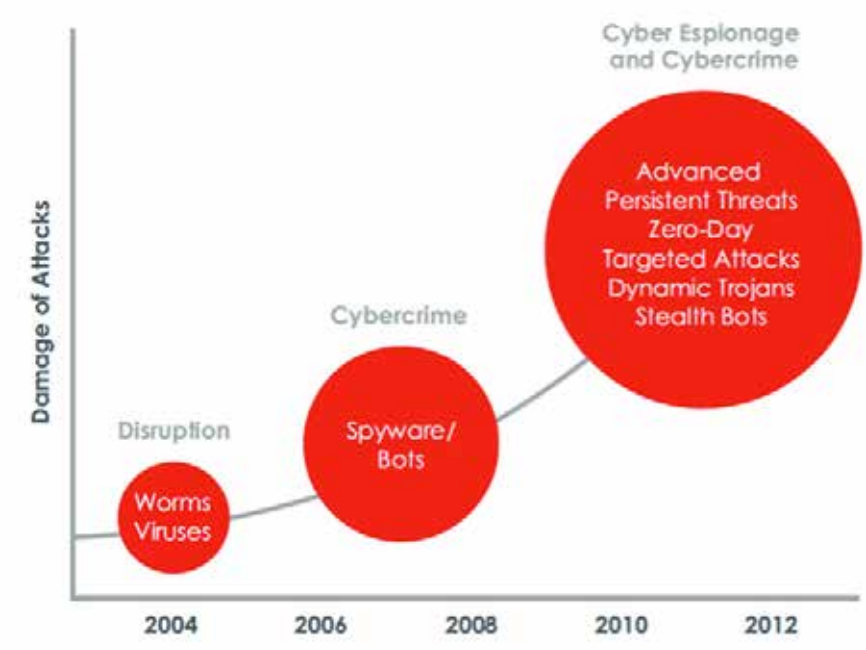
The Problem

SME's, Enterprises and government agencies are under virtually constant attack today. There have been significant breaches at RSA, Global Payments, ADP, Symantec, International Monetary Fund, and most notably Sony. Undoubtedly thousands more have occurred that we haven't even heard about. Flame, Stuxnet, and a number of other cyber attacks have been uncovered that set an entirely new standard for complexity and sophistication.

Fundamentally, these developments make clear that the cybercriminals, nation-states, and hacker activists waging these attacks are growing increasingly sophisticated and more effective in their efforts to steal and sabotage. Leveraging dynamic malware, targeted spear phishing emails, elaborate Web attacks and a host of other tactics, these criminals know how to bypass traditional security mechanisms like firewalls and next-generation firewalls, IPS, anti-virus (AV), and gateways. Think your organization is immune? If so, it's in the vast minority: ninety five percent of organizations are routinely compromised, with the theft of intellectual property, customer records, and other sensitive data increasingly common.

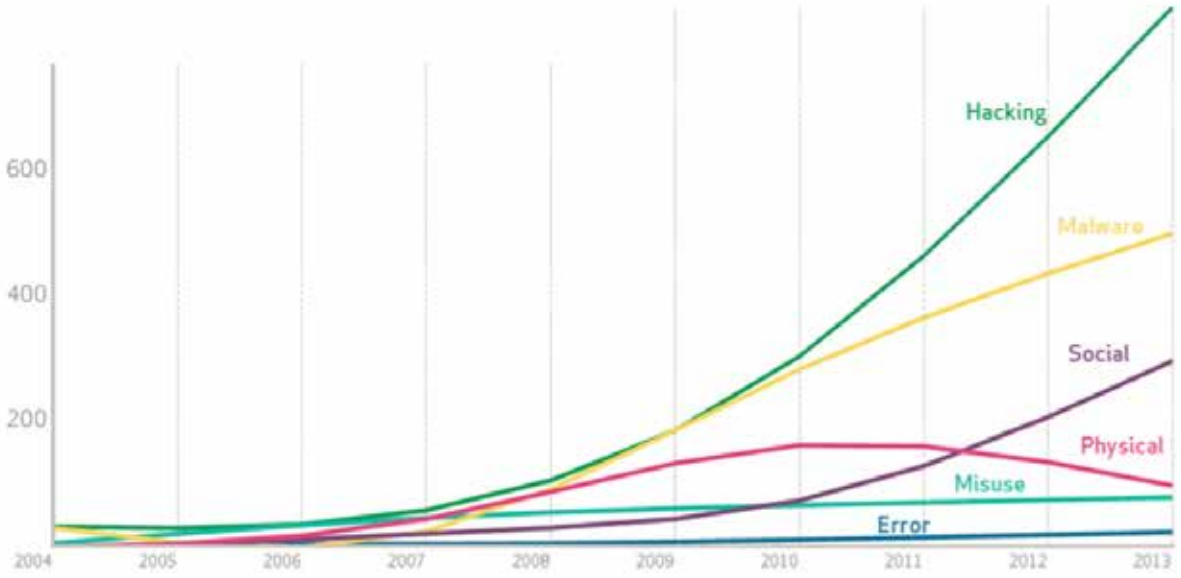
Here's how a 2012 Gartner report put it: "There is widespread agreement that advanced attacks are bypassing our traditional signature-based security controls and persisting undetected on our systems for extended periods of time. The threat is real. You are compromised; you just don't know it."

Below shows the changing agendas of Cyber Attacks over time:



Between 2003 and 2013 Verizon looked into 92,000 security breaches.

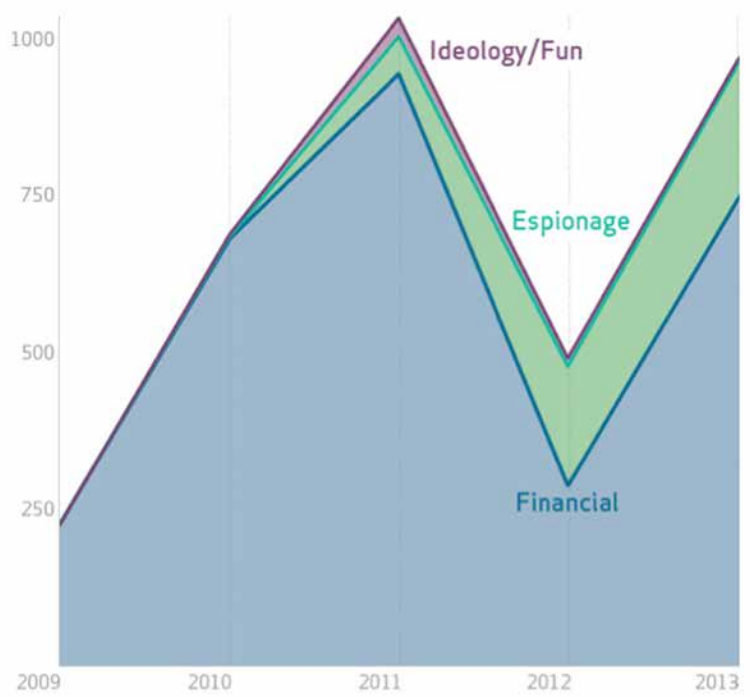
Number of breaches per threat action category over time



As you can see, Hacking has grown exponentially. In addition much of the Malware and Social attacks were simply the first phase in a hack. The growth of hacking can be attributed to the monetization of cyber-crime. The graph to the right from the same study shows the motivation behind these attacks.

As you can see the overriding motivation is financial. In this case information is either stolen and sold or held for ransom. A second motivation is espionage, a famous example being Sony pictures.

Number of breaches per threat actor active over time



BIOS
desktop to datacenter

WHY YOU SHOULD CARE

If your organization is like most you are spending a lot of money, perhaps 10-20% of your annual IT budget, on security—but it's not working against the new breed of advanced cyber attacks. If that's not enough to concern you consider how losing the security battle can hurt your business:

Loss of competitiveness.
When cybercriminals can circumvent your defenses, trade secrets, patents, customer records, and M&A activities can all be exposed and significantly weaken your competitive position.

Compliance breaches
If you are not protected from breaches, your organization's compliance with relevant policies and mandates is in serious jeopardy. Whether you are a financial institution that needs to safeguard credit card data and stay compliant with PCI DSS, or your business is tasked with compliance with HIPAA, NERC, FISMA, privacy rules, or any of the other policies in effect around the world, data breaches can lead to fines, lost business, and a host of other penalties.

Damaged reputation
Customer trust and market share are precious commodities. All it takes is a significant breach to hit the headlines, and those hard-earned assets can erode quickly. Estimates from companies that have been breached have ranged in the several millions of dollars up to 200 million dollars.

Lost productivity
If your security team is finding out about breaches after the fact, they are going to be scrambling to handle forensics, shore up the vulnerability, assess where other similar gaps may be, rebuild corrupted systems, and so on. The time spent on these efforts is time your business doesn't get back—and that can't be focused on more strategic efforts.

WHY ARE TODAY'S SECURITY DEFENSES FAILING?

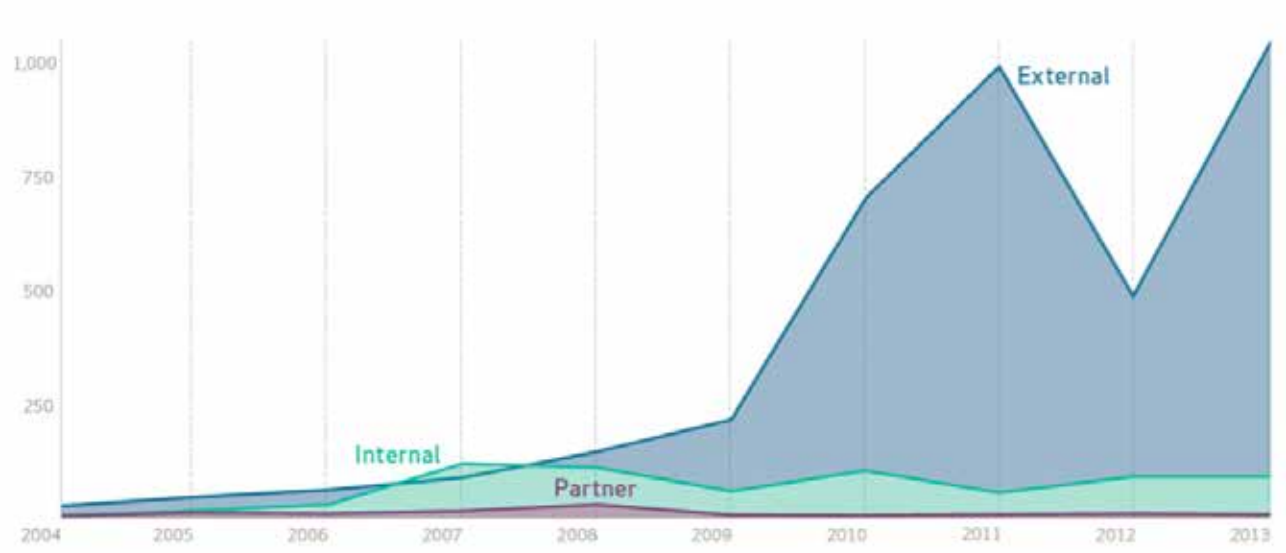
In this battle, IT & IT Security teams are using an outdated arsenal: legacy security platforms based on technology that originated many years ago using signatures. These tools are good at blocking basic malware that is known and documented, such as viruses, but they are incapable of identifying today's dynamic, multi-pronged cyber-attacks, which are often called advanced malware or advanced persistent threats (APTs). Companies with more advanced Security are using behavioral tools designed to prevent zero day attacks which is more effective then legacy security platforms. However all these security devices, old or new fail to provide IT and Security teams with two vital pieces of information?

Firstly: what can the hackers see?

Humans make mistakes. Yet in almost all companies we deal with non-have ever externally scanned their environment to quality check the configuration, architecture or software level of their externally facing infrastructure. One mistake, firewall that isn't updated or unpatched server could undo the whole effort.

The diagram below shows the origin of security breaches. As you can see more then 90% are from external threats.

Number of breaches per threat actor category over time



Secondly, IT & Security Teams need to know when a breach occurs!

In the case of the Sony Pictures, hackers gained entry months before they announced to the Sony staff that they had been hacked. After gaining initial entry they moved horizontally through the network capturing Administrator and User credentials without detection. Over a period of many months they extracted TB's of data from Sony including all their emails, Staff Salary information and unreleased movies. They then destroyed all Sony's backups and then erased all their data leaving only a skull and cross bow on each staff members PC Finally they published all the companies secrets online leading to the resignation of the CEO and other C level staff. The fact that Sony had no idea they had been hacked for months is what made this hack so damaging. Had they been hacked and been able to identify the breach within hours or days, they would not have suffered such horrendous damage to their brand and their company.

TB's of data were extracted over many months. At no point was the Sony IT team aware.

BIOS
desktop to datacenter

WHAT CAN YOU AS A 'C' LEVEL EXEC DO?

Firstly, allow your team to see what hackers can see:

Undertake an external vulnerability assessment from BIOS so we can show your teams what the hackers can see.

Once fixes and patches and changes are applied to close the gaps take a Internal and External Continuous Vulnerability Scanning from BIOS. This will allow your team to know what patches are needed on an ongoing bases, allow them to be aware of any configuration mistakes and provide them with up to date intelligence. Your team will also have access to our Security team and monthly in-depth and management reporting. All for a low fixed monthly cost.

Secondly, give your team the service to know if a breach occurs:

Take a SIEM (Security Incident Event Management) Service from BIOS. This will allow us to alert your team should any incents occur. Our Security Operation Center operates 24x7 and will work diligently with your team off and on site to address any security concerns.

To see if your company qualifies for a free one off Vulnerability Assessment contact us today on 800 BIOSME or visit www.biosme.com