Cybersecurity in the boardroom

Practical support for executives in a world where cyber attacks and defenses are automated

White paper
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The worst shock most CEOs will ever experience</td>
<td>3</td>
</tr>
<tr>
<td>Why now, why me?</td>
<td>4</td>
</tr>
<tr>
<td>What happens in the boardroom?</td>
<td>5</td>
</tr>
<tr>
<td>Failing to plan = Planning to fail</td>
<td>6</td>
</tr>
<tr>
<td>Why security orchestration is needed</td>
<td>7</td>
</tr>
<tr>
<td>How hackers view your business</td>
<td>8</td>
</tr>
<tr>
<td>Sources of quotes and statistics</td>
<td>10</td>
</tr>
<tr>
<td>About the Cyber Rescue Alliance</td>
<td>10</td>
</tr>
<tr>
<td>About the Nokia Threat Intelligence Lab</td>
<td>11</td>
</tr>
</tbody>
</table>
The worst shock most CEOs will ever experience

In the search for profit, executives have demanded data lakes and digital oceans, using information as their compass, their cargo and their fuel. But if data is the energy of the digital economy, it follows that data breaches can be explosive.

Most CEOs are unprepared for a major data breach. Over a third are unaware of the worst cyber incidents their teams handled this year. More than forty per cent wrongly think their insurance covers cyber attacks. Less than half have a plan for the commercial consequences of a major breach. Just one in ten has rehearsed for the inevitable.

Leadership is needed, from business executives who are ready to protect reputation and revenues from future cyber attacks. Progressive leaders will invest in three areas:

1. **Commercial simulations of breach response in the Boardroom (page 5)**
   Rehearing for the shock, speed and ambiguity of a successful cyber attack helps executives avoid mistakes made by their peers. Simulations show where investment in risk mitigation will give the best return, for corporate resilience and breach recovery.

2. **Security automation and orchestration (page 8)**
   A single cohesive end-to-end management solution is essential for effective response to accelerating threats. Enterprises must be able to prevent, pinpoint and address security threats in a cost-efficient and timely manner.

3. **Independent scorecard of how hackers view your business (page 10)**
   Security managers check physical security by walking around key buildings, looking for vulnerabilities that criminals can see from the outside. Those daily checks must be replicated online, with automated reports on cyber vulnerabilities staff haven’t closed.

Simulating a major breach is the best way to help leaders internalize the business nature of the cyber threat. Just ninety minutes invested in rehearsing a major breach can also transform a Board’s appreciation of IT security. Intense simulations show executives how they will be personally responsible for leading business recovery after a breach. Leaders can only avoid mistakes made by other organisations if they have rehearsed how to do so.

Security automation and orchestration are essential for protecting an organisation’s reputation as well as its data. This is particularly true during a breach, as most CEOs have unrealistic expectations about how fast breaches will be identified and fixed. In typical companies, only 30% of cyber security incidents are investigated, and of those, 70% are false positives. Without automation and orchestration within IT Security, many Boards will be disappointed at their time of greatest need.

Independent scorecards are used to judge performance in most key areas of business. Directors can easily find out “where we rank on the stock market,” and “how our executive pay compares to our peers.” Finance Directors buy reports on credit ratings and Marketing Directors pay for reports on market share. Chief Risk Officers and Security Directors should be able to rank themselves just as easily on cyber, as cyber vulnerabilities change so fast.

In the next decade, most CEOs will need to orchestrate business response to a major data breach. Leaders can minimise the shock and damage of such a breach, by preparing now.
Why now, why me?

Computers will never be safe, according to the front page of The Economist\textsuperscript{08}. But executives have been slow to hear that message, as they are more likely to ask “when will our new app launch” than “is our new app really secure?”

The IT Directors who build new apps are under pressure to be fast and flexible. Few Boards really appreciate the risks that such pressures create. The truth is that most Directors are not aware how quickly the risks are growing for any business connected to the internet.

The number of internet connections at each business is growing exponentially, as companies invest in mobility, connectivity and the Internet of Things.

Every connection to the internet is part of a growing “attack surface” that hackers can exploit. Criminals have automated the development of software to attack every internet-connected device, for example producing over 6 million different malware variants to target mobile phones in 2017\textsuperscript{09}.

Many executives don't appreciate the scale of the problem, because the vast majority of attacks have been kept secret. In the UK, a major survey found that 95% of businesses keep their most disruptive data breaches from the public, including 82% who don't report breaches to the police\textsuperscript{10}. That secrecy makes it hard for other businesses to appreciate how much the digital world has changed. The compound growth rates of some types of attack should focus minds. The last year has seen a 27.5% annual growth in data breaches reported by businesses\textsuperscript{11}; a 2,000% increase in ransomware attacks\textsuperscript{12} and an 8,500% increase in cryptojacking of computers\textsuperscript{13}.

“Why us?” is a frequent response when a major breach occurs. Emotions affect judgement just when rational reflection is most needed. Here’s how some leaders have reacted to a breach:

<table>
<thead>
<tr>
<th>I am incredibly angry about this data breach\textsuperscript{14}</th>
<th>I had no intuitive idea how to move forward\textsuperscript{15}</th>
</tr>
</thead>
<tbody>
<tr>
<td>John Legere, T-Mobile USA</td>
<td>Soren Skou, CEO, Maersk</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>I realized there was nothing at all that I could do\textsuperscript{16}</th>
<th>I've been through stages of denial, disbelief, frustration\textsuperscript{17}</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amy Pascal, ex-CEO at Sony</td>
<td>Robert Pera, CEO, Ubiquiti Networks</td>
</tr>
</tbody>
</table>

CEOs need to be prepared for the increasing volume and sophistication of attacks on their business. Rehearsing their leadership team is an excellent investment\textsuperscript{18}. 

\textsuperscript{08} The Economist
\textsuperscript{09} 2017
\textsuperscript{10} Survey
\textsuperscript{11} 2011
\textsuperscript{12} 2016
\textsuperscript{13} 2017
\textsuperscript{14} John Legere
\textsuperscript{15} Soren Skou
\textsuperscript{16} Amy Pascal
\textsuperscript{17} Robert Pera
\textsuperscript{18} Rehearsal
What happens in the boardroom?

Major cyber attacks are a low probability, but very high impact event. They can damage personal as well as corporate reputations. Share prices move when large breaches are announced, and they move again when investors reflect on how well executives have led the response.

Leaders rehearse for crises of many types. In most countries, it's a legal requirement to practice for an office fire at least once a year. Such fires can kill, and 17 people died in fires across all the UK's factories, farms and offices last year\(^{19}\). Data breaches are almost never not deadly, but they happen at a far greater rate and can lead to company bankruptcy.

A good boardroom simulation of a major data breach tests internal command and control, commercial judgement and coordination. Executives learn where data assets are held, how they may be compromised, and the resources needed to protect them. A good simulation is a challenging, visceral experience. Participants leave with a greater appreciation of their own responsibilities, and a desire to ensure that colleagues have the tools they need.

Some of the insights that a Boardroom simulation of a data breach should expose include:

**The shock of a breach** is often made worse by several factors. For example, you may be told of this Breach by an outsider, most frequently by Law Enforcement (41%) or Third Parties including customers (35%)\(^{20}\). You may then discover you weren’t told of previous Data Incidents. Often, you are weeks behind the attackers, as the average time to discover a breach is 66 days (followed by 36 days of forensics)\(^{21}\).

**Help from authorities** is easier if you already know the right people. But who? There are 31 organisations fighting cyber threats to Financial Services in the UK\(^{22}\), where 68% of Directors are unaware of who to call\(^{23}\).

Some authorities have less resources than they’d like. The UK’s ICO has 30 officers handling 200,000 concerns and 1,000 cases per year\(^{24}\). UK police spend under £20 per person on cybercrime training\(^{25}\).

**Your chain of command** will be stressed by ambiguity during a suspected breach. The UK Parliament is clear on who should lead cyber response in a business\(^{26}\).

Opinions may fill the gap where facts are missing. Only 45% of security professionals are confident they can determine the scope of a breach\(^{26}\). External forensics typically lasts 36 days\(^{27}\). And decisions must be made fast: 91% of consumers expect “24 hours or less.”\(^{28}\)

**Your legal and moral responsibilities** might not be immediately clear. For example, law enforcement may ask you not to notify customers, so that the hacker won’t be alerted to their investigations.

Extra-territorial laws on protection of citizens from cyber attack make you subject to the requirements of more countries than you operate in. A summary of Privacy & Breach laws runs to 500 pages\(^{29}\).

**Serious decisions require money.** In the UK, 52% of CEOs think they have cyber insurance, but <10% do\(^{30}\). Some 81% of companies with cyber cover in USA have never claimed on it\(^{31}\). Claims may be needed on a wide variety of cost categories\(^{32}\).

**Will you pay for a big gesture?** 60% of Breach Notifications offer Credit Monitoring\(^{33}\). And what of the long term revenue impact? Abnormal churn after a breach ranges from 6.2% in Financial Services and 5.3% in Health, down to 0.1% in Public Sector\(^{34}\).

**The surge** in enquiries can quickly turn into more irate calls from customers who—in their moment of crisis—want to receive the global standard in call centre response, 80% of calls answered in 20 seconds.
But after a breach, call volumes can be one hundred times higher than normal. And in addition, you must communicate with Regulators, Suppliers, Press, Staff, Police and Shareholders, and manage Social Media.

**You will be criticised**, even if your company suffered a criminal attack. Customers complain you notified “too slowly … too fast … without cause … putting us at risk of scammers.” Consumers say “Credit Monitoring doesn’t help me” or “How will you make this good” or simply “I want to break my contract and leave.”

The UK Parliament has called for bigger fines for poor response and a cyber impact on CEO bonuses.

Participants in a simulation need to be relaxed enough to learn, but challenged enough to be stretched. Friendly competition can energise participants, and create a little pressure. A good simulation is an opportunity to learn, to bond and to reflect. It encourages reflection on how to avoid—and mitigate—a breach.

**Failing to plan = Planning to fail**

A key lesson from every cyber attack simulation is the need for a plan. All large enterprises have a continuity plan, but too many assume that it covers the challenges of modern cyber attacks.

In fact, a breach often reveals disagreement about such basics as “what is cyber security for.” Two thirds of Board members consider Brand Protection to be a top priority of cyber security, yet less than one in five security professionals understand this.

A bespoke business response plan helps executives lead recovery, by avoiding the mistakes that others have made, and by clarifying the areas of responsibility for each person.

Going into battle, fighting to save your reputation and revenues during a major hack, is like boxing an invisible opponent. You can’t assume that the crisis management plan you’ve written for situations like a fire or a pandemic will work against a cyber attack. We sometimes quote what Mike Tyson used to say, of his over-confident opponents: ‘everyone has a plan, until they get punched in the face!’

A customised commercial response plan, prepared in advance of a major data breach, will make your response much more timely and effective. It provides Directors with simple checklists, templates and instructions about each of the decisions they must face. Crucially, it will document where sensitive data is held, including by third party suppliers and information processors, so that breaches caused by partners are considered during the initial forensic stage of response.

The plan has to be easy for executives to use. A section has to be provided for each executive, highlighting the resources they can call upon, the consequences of alternative actions they must choose between, and even the text of communications they may need to issue very urgently.

Source: Cyber Rescue Alliance
Why security orchestration is needed

The Ukraine has been something of a test laboratory for hackers. The country has suffered two major attacks on its power distribution grid in subsequent years—2015 and 2016. More recently, in 2017, the ‘Petya’ ransomware attack began with infections of organizations working with the Ukrainian government, including banks, state power utilities and Kiev’s airport and metro system, quickly spreading worldwide and hitting systems in many countries.

The attacks show that cyber attacks are a growing threat to any digital network and their operations. It’s been said there are two kinds of organization—those who are aware of having been hacked and those that still have not found out.

It’s a real and present danger that causes financial loss, but more importantly compromises the safety of people. Networks, communications and data simply cannot be allowed to fail when safety is at stake.

As organizations and their boards are increasingly depending on services and data, CEOs and their Boards need to know that their enterprise security is being led effectively. With the rapid growth of new attacks, this requires an investment in security automation and orchestration.

While cyber criminals are excellently connected, permanently working on how to automate cyber attacks to increase efficiency, in today’s security operation centers 33% of incident response time is still spent on manual processes each day. Combined with data deluge and alert fatigue, resulting from the fragmented nature of the security market with a myriad of point tools each with its own administration, management, and reporting capabilities, considerable time is wasted on false positives, while real breaches go undetected.

Security teams are also challenged by new threats and increased attack surface due to complex technology and business transformations such as cloud, IoT and 5G, which worsens the fact-based information to the board on real risk situation.

CEOs and their board members need today a security analytics enabled ACTIVE Security to detect indicators of compromise, proactively identify harmful actors, help security teams prioritize risks, and initiate appropriate rapid response. Nokia’s NetGuard ACTIVE Security provides a contextual risk management dashboard (and if still needed printed reports) of security posture across the complex, heterogeneous, and diverse operational environments.

Active security enables companies to streamline processes, accelerate decision-making and optimize costs while preventing, identifying and addressing security risks and threats before they result in data breaches or worse.

Rapid technological developments lead to an enormous dependence of enterprises on the information and communication technology. CEO’s concerns are rising on how to manage the security risks to ensure that at all times an organization can continue operating to at least a pre-determined level.

A holistic Security Orchestration, Automation and Response (SOAR) solution does identify potential threats to large multi-vendor networks and services as well as their impacts to business operations, and provides a framework for building resilience and the capability for an effective response. NetGuard ACTIVE Security is a key enabler for transforming security organizations from manually driven operations to intelligence driven security operation centers based on automation. NetGuard ACTIVE Security is a security operations automation, analytics and reporting platform that consolidates data and extracts actionable insights from a variety of intelligence sources, and existing security technologies. By analyzing user behavior to identify bad actors, it provides threat indicators to potential insider threats. These capabilities help security professionals prioritize risks and automate security operations activities in the context of the attack surface and the business.
Hardly a day goes by without the media reporting a cyber security breach or exposure of a risk somewhere in the world. Not only are attacks becoming ever-more sophisticated, but the potential damage that can result is growing, even physical damage to infrastructure such as electricity distribution grids.

Companies and their IT can ill afford any successful hacks. Not just financial loss is at stake; lives can be put in jeopardy.

Implementing the right level of security is a high priority. Consequently, cyber-security must be stepped up. Key capabilities to secure networks include security automation that encompasses business processes, regulations and policies; end-to-end security that encompasses the operation of the network and its processes; security analytics to correlate data from across the network, devices and cloud layers to spot suspicious anomalies and provide insight into threats; and multi-layer encryption to protect data.

Such an active security approach provides the right balance of costs with the in-depth protection needed to defend against toady’s security threats.

How hackers view your business

Traditional security directors build physical security through locks, barriers, training and processes. Then they walk around key premises to spot the open windows a criminal might still exploit. That external perspective is essential for cyber security.

Nokia has made an investment in Security Scorecard, which uses proprietary technology to identify the vulnerabilities that external hackers can exploit at each specific enterprise.

Chief Risk Officers find such information helps them to independently assess, monitor and report on how cyber risks are evolving at their organisation. Consider the graph below, showing how cyber vulnerabilities can change over time.

The graph shows how the number and seriousness of vulnerabilities at one (very large) bank changed during 2017. If you were the CRO at this bank, you might ask yourself “Was I aware of the collapse in our cyber security between May and June?”

New cyber vulnerabilities arise daily, for example when a company updates its systems, makes an acquisition or brings on a new supplier. Risk increases when hackers start to chat about a company, or when a social engineering campaign targets the business.
Chief Risk Officers should be able to see the trends and details of how they compare to similar organisations. The graph below summarises the Security Scorecard of 60 banks over 30 days.

Source: Cyber Rescue Alliance

Analysis by SSC has shown that businesses with a security score below 70% are five times more likely to suffer a breach than companies with a score above 90%. Business leaders should be asking to see how their business (and their suppliers) perform on such scorecards of the vulnerabilities visible to hackers.
Sources of quotes and statistics

The original source of each statistic referenced in this white paper is available by clicking each annotation number in the pdf version of this report.

Alternatively, the reports are available in the Cyber Rescue library: https://www.cyberrescue.co.uk/library/threat

For further information, contact Assistance@CyberRescue.co.uk

About the Cyber Rescue Alliance

The Cyber Rescue Alliance exists to reduce harm caused by cyber attacks on businesses.

Cyber Rescue helps CEOs, CxOs, CISOs and IT Directors to anticipate and respond to the cascade of commercial consequences that follow a major data breach.

Services include:

• **Executive Simulations of Cyber Attacks.** We deliver a visceral experience of the shock and uncertainty that arrives with an alleged data breach. We demonstrate the cascade of commercial challenges, to inoculate decision makers from mistakes that others have made during a breach.

• **Commercial Response Plans for Cyber Attacks.** These bespoke documents include decision trees and scripts needed by each functional director, including Customer Services, Operations, Legal, HR, Finance, PR, IR, IT and Business Continuity. We integrate your cyber attack response plan into your existing Business Continuity Plan.

• **Cyber Crisis Coaching to the executive team.** During the golden hour at the start of your commercial response to a major cyber attack, an experienced Crisis Coach is invaluable. This is when you establish command and control, stand-up your response team, triage business issues, identify uncertainties and set priorities.

Find out more about the Cyber Rescue Alliance, at:

• [https://www.cyberrescue.co.uk](https://www.cyberrescue.co.uk)
• [https://www.linkedin.com/company/cyber-rescue-alliance](https://www.linkedin.com/company/cyber-rescue-alliance)

**To schedule a conversation** about this white paper, contact Assistance@CyberRescue.co.uk

Please contact the main author of this paper at Cyber Rescue: Kevin.Duffey@CyberRescue.co.uk

Cyber Rescue and Cyber Rescue Alliance are trademarks of Cyber Rescue Ltd. Cyber Rescue, 9 Devonshire Mews, London, W4 2HA, United Kingdom. Tel: +44 (0) 207 859 4320
About the Nokia Threat Intelligence Lab

The Nokia Threat Intelligence Lab focuses on the behavior of malware network communications to develop detection rules that identify malware infections based on command-and-control communication and other network behavior. This approach enables the detection of malware in the service provider’s network and the detection rules developed form the foundation of the Nokia network-based malware detection product suite.

To accurately detect that a user is infected, our detection rule set looks for network behavior that provides unequivocal evidence of infection coming from the user’s device. This behavior includes:

- Malware command-and-control (C&C) communications – Backdoor connections
- Attempts to infect others (for example, exploits) – Excessive email
- Denial of Service (DoS) and hacking activity. Four main activities support our signature development and verification process:
  - Monitoring of information sources from major security vendors and maintaining a database of current and active threats
  - Collecting malware samples (>200,000/day), and classifying and correlating them against the threat database
  - Executing samples that match the top threats in a sandbox environment and comparing them against our current signature set
  - Conducting a detailed analysis of the malware’s behavior and building a new signature, if a sample fails to trigger a signature

Find out more about the Nokia Threat Intelligence Center, visit our Security solution page, or learn more about the Nokia NetGuard Endpoint Security solution.