GOLDMAN JUDIN INC.
ATTORNEYS
Reg No. 1998/011/368/21

Wanders Office Park
Pavilion Building Second Floor
52 Corlette Drive
Illova

PO Box 78662 Sandton 2146
Docex 264 Randburg

e-mail: law@elawnet.co.za
website : www.gji.co.za
tel: +27 (11) 595 2300

Warning of More Cyber Attacks

23 January 2013 - the Chicago Tribune reports that the FBI has warned US retailers to prepare for more cyber-attacks after discovering about 20 hacking cases in the past year that involved the same kind of malicious software used against Target Corporation of the US in the holiday shopping season just passed.

The US Federal Bureau of Investigation distributed a confidential, 3-page report to retail companies recently describing the risks posed by "Memory – parsing" malware that affects point-of-sale (POS) systems which include cash registers and credit-card swiping machines found in store checkout isles.

In an excellent article Ed Batts, a leading US lawyer in the field of cyber security writes that as directors prepare to fulfil their duty of care in an informed way, what are the issues that matter today? He has created a checklist to help outside directors understand the cyber security issues that matter to boards today based on information from panel discussions and individual directors:

1. Who's in charge? Who is the company's Chief Privacy Officer and Chief Information Security Officer? What are the charters and functions of each position, and what is the interaction between the privacy compliance and information security teams? Is there a check-and-balance on the Chief Information Officer – for instance, is the CISO and CTO one and the same person, or are these responsibilities divided, and does the CISO report to the CIO or have an alternate potential reporting route?

2. What is the role of board oversight? Who is the lead director on information security and is that position informal or formal? Is at least one outside director sufficiently technically educated to be able to lead board discussions and questions on information security? Does information security oversight rest with the Audit Committee and, if so, is it part of the Audit Committee annual work plan? Does the Audit Committee in practice actually regularly review information security issues?

3. Who are your likely adversaries? Who is most likely to want access to the company's systems? What level of sophistication, geographic scope and motives (e.g. economic/embezzlement, identity theft, trade secret theft) may these adversaries have?

4. Does the company have an incident response plan? What are the protocols for informing customers, suppliers, internal constituencies and regulatory bodies (including SEC reporting) on information security incidents? Has the company identified relevant internal and external

(such as technical, legal, public relations) core team members? Has the company set up liaisons with law enforcement authorities?

5. What are the BYOD protocols? Is the company a bring-your-own-device (BYOD) environment? If so, what the level of safeguards is applied to such devices?

6. What does the network map of the company look like? What data is stored on which servers and controlled by whom? Does the company triage/organize server storage functions? What information security functions are provided by contractors, and what is the level of assurance in the integrity of those contractors?

7. Has the company assessed the inside threat? What access and administrative rights exist? Does the company have a policy on thumb/USB drives or other mass storage devices and use/scanning? Does the company monitor internal networks for inappropriate file access or sharing?

8. What is the interplay between physical and cyber security? Does the company actively manage both physical and cyber security? What physical security measures are used to enhance cybersecurity? What procedures exist for terminated employees' deactivation?

9. How does the company interact with suppliers, customers and partners? To what extent does the company provide products "downstream" that if compromised or misused would affect the company? How the company is assured that third-party solutions, including software, are free of issues and include indemnification for potential flaws?

10. What insurance does the company carry for cybersecurity? What are the policy limits and exclusions on insurance coverage?

Given section 76 of South Africa's new Company's Act, the looming threat of class actions and the regretful fact that in South Africa many entities have not prepared for cyber-attacks, the checklist above is of critical and vital importance and, with respect, should find its way onto the agenda of every entity, whether a public company, a private company or any other entity of whatsoever nature or kind. In our opinion, every director and prescribed officer who fails to give this issue the critical importance which it deserves does so at their own risk and peril and could find that not even their insurance is there to assist in the event of an attack and the substantial financial and reputational loss which invariably follows such an event.

Prepared by Michael Judin of Goldman Judin Inc.

Michael may be contacted on +27 (0) 83 300 5000 or at michael@elawnet.co.za