A Leader's Guide to Cybersecurity

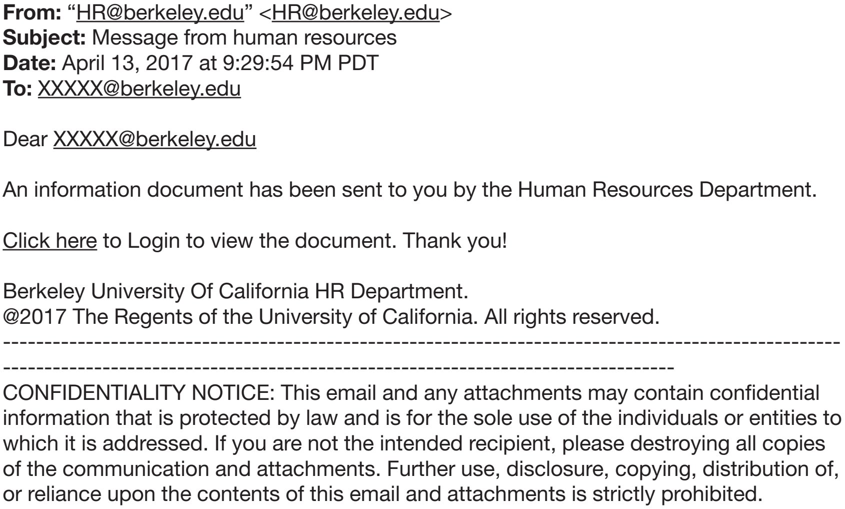
Why Boards Need to Lead—And How to Do It

By Thomas J. Parenty and Jack J. Domet

Contents

FIGURE 1-1

Example of phishing attack



From: "HR@berkeley.edu" <HR@berkeley.edu>
Subject: Message from human resources
Date: April 13, 2017 at 9:29:54 PM PDT
To: XXXXX@berkeley.edu

Dear XXXXX@berkeley.edu

An information document has been sent to you by the Human Resources Department.

Click here to Login to view the document. Thank you!

Berkeley University Of California HR Department.
@2017 The Regents of the University of California. All rights reserved.

CONFIDENTIALITY NOTICE: This email and any attachments may contain confidential information that is protected by law and is for the sole use of the individuals or entities to which it is addressed. If you are not the intended recipient, please destroying all copies of the communication and attachments. Further use, disclosure, copying, distribution of, or reliance upon the contents of this email and attachments is strictly prohibited.

TABLE 1-1

Sample of ongoing cyber vulnerabilities

Topic area	Specific concern	Relevance today
Files	Theft, copying, and unauthorized access to sensitive information	This is still one of the most significant cyber risks organizations face.
Software	Failure of protection features, including control over what information people can access	In most cases of insider theft of company information, a failure of access controls facilitated the theft.
Users	Weak authentication of computer users	Criminals impersonating users, often through the use of stolen passwords, continue to haunt both companies and individuals.
Network communications	Ability to tap and intercept network traffic	The risk still exists, but fortunately encryption solutions are widely deployed.
System administration	Administration mistakes resulting in compromise	One of the major risks of the internet of things and the expanding adoption of technologies outside IT department control is that the users of these devices do not know how to manage them securely. In addition, many of the breaches of corporate information stored in the cloud are due to configuration mistakes.
Programmers	Programmers modifying their software to disable security features introduce back doors and otherwise subvert security	All these concerns currently exist.

TABLE 8-1

Four elements of cyber threat narratives

Element	Purpose
Critical business activity and risks	Identification of a critical business activity and the risks it faces
Supporting systems	Identification of the computer systems on which a business activity relies
Cyberattacks and consequences	Cyberattacks that can cause critical business activity risks to materialize and their impact
Cyber adversaries	Identification and characterization of likely attackers

TABLE 8-2

Four elements of cyber threat narrative at Maroochy Shire

Element	Maroochy Shire example
Critical business activity and risks	Activity: Wastewater treatment Risk: Pumping station malfunction
Supporting systems	Centralized operations management system Pumping station control equipment
Cyberattacks and consequences	Exploitation of insecure network communications and lack of user authentication on pumping station control equipment Massive release of raw sewage
Cyber adversary	Disgruntled former employee