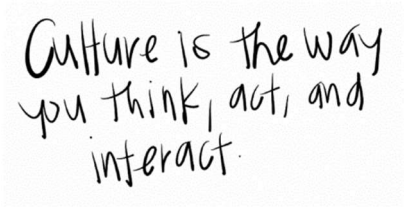
Tips for CFO: Mitigate against spear-phishing and whaling (C-Level Targets) cyberattacks

People

People considerations need to be factored into your cyber risk mitigating strategy. Sophisticated technologies, security and technical expertise and well-defined procedures alone are insufficient for an effective strategy. Proper training programs and addressing your organization's attitude towards security is necessary to ensure your multi-layered strategy will be effective.

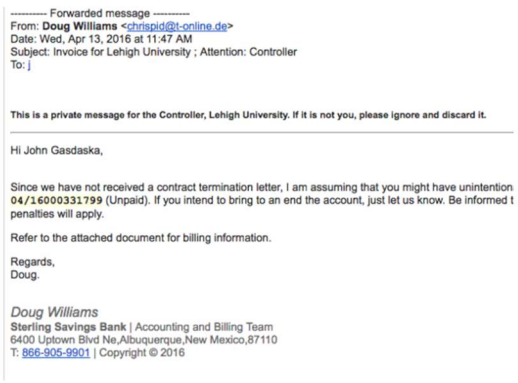
Training employees about data privacy and security is critical. 56% (up from 38% in 2015) of attacks use a method called phishing where employees are tricked into clicking an email link to give hackers access to corporate systems and data. Take University of California Davis Health's incident in May of this year as an example. An employee who responded to a phishing email allowed a hacker to obtain data that compromised 15,000 patients' personal health information (PHI). Had the employee been educated to identify characteristics of a phishing email, this attack could conceivably have been avoided.



Cultivation of the right (employee) attitudes and behaviors is just as important. Employee-training (particularly in the Finance Department because users and executives have valuable login credentials that access bank accounts, treasury and financial systems), combined with the reinforcement of the right behaviors is key to improve a company's overall security posture. The responsibility for data security cannot be contained to just the CISO or security team. Like good citizens of a society, it is everyone's responsibility to recognize and report illegal or suspicious activity, and a company's employees and contractors can and should be able to do the same. Training is necessary to help employees and workers identify suspicious activities or behaviors. This includes executives, who are often primary targets of whaling and spear-phishing attacks. **Consider organizing and implementing externally provided professional spear-phishing and whaling (executive and C-level) training, which is in expensive to do.**

Examples of real-world spear-phishing and whaling incidents.

11. Sent "From" Recipient's Bank



---------- Forwarded message ----------
From: **Doug Williams** <chrispid@t-online.de>
Date: Wed, Apr 13, 2016 at 11:47 AM
Subject: Invoice for Lehigh University ; Attention: Controller
To: j

This is a private message for the Controller, Lehigh University. If it is not you, please ignore and discard it.

Hi John Gasdaska,

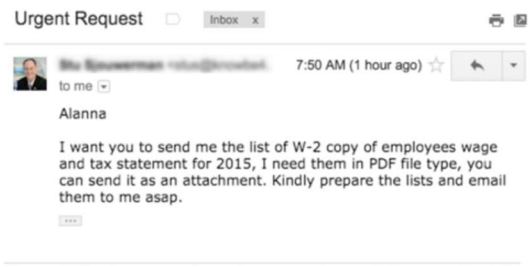
Since we have not received a contract termination letter, I am assuming that you might have unintention
04/16000331799 (Unpaid). If you intend to bring to an end the account, just let us know. Be informed t
penalties will apply.

Refer to the attached document for billing information.

Regards,
Doug.

Doug Williams
Sterling Savings Bank | Accounting and Billing Team
6400 Uptown Blvd Ne,Albuquerque,New Mexico,87110
T: 866-905-9901 | Copyright © 2016

14. Sent "From" Recipient's CEO



Urgent Request Inbox x

[redacted] 7:50 AM (1 hour ago)
to me

Alanna

I want you to send me the list of W-2 copy of employees wage and tax statement for 2015, I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me asap.

17. Sent to Controller "From" Their CEO (Also CCing Their Accountant)

To: ACCOUNTING DEPARTMENT
Cc: TomHeald@strategictax.com
Subject: W2's for All Employees
From Tom Smith Signature: None

Please send our W2 Tax Documents for all employees to Tom Heald at Strategic Tax Consultants. I have cc'd him here.

We need these documents for a review ordered by the Board of Directors.

Please send immediately as we are under a time crunch.

Thanks,

Tom Smith
CEO
BetterSystems Inc

16. Sent to VP "From" Their CEO

[redacted]
To: [redacted]
Reply-To: [redacted]
Payment
13 July 2016 at 9:38 AM
IJ

Hi Michael,

Please find enclosed vendor banking instructions for a payment that was suppose to go out in the previous week. I need you to process it immediately.

I am a bit busy now but will give you a call within the hour regarding the payment.

Regards,

[redacted]

Sent from my Mobile

