Volume 5, Issue 7
July 2023

TLP:CLEAR

FB-ISAO Current Threat Level

FB-ISAO Physical Threat Level:
Guarded

FB-ISAO has assessed the general Physical Threat Level for US Faith-Based Organizations as **"GUARDED."** As per FB-ISAO's definitions of the Physical Threat Levels, **GUARDED"** means FB-ISAO is unaware of any specific events, but a general risk of incidents exists.

FB-ISAO Cyber Threat Level:
Guarded

FB-ISAO has assessed the general Cyber Threat Level for US Faith-Based Organizations as **"GUARDED."** As per FB-ISAO's definitions of the Cyber Threat Levels, **"GUARDED"** means FB-ISAO is unaware of any specific events, but a general risk of incidents exists.

Stories

FB-ISAO Newsletter

Managing Out of Office Notices

Ah! Here it is! Time to enjoy everything that summer has to offer, which includes vacations, holidays, or general personal time-off work. When preparing to leave work behind for some much-needed time off, we certainly want to make sure all our ducks are in a row, including advising leadership and colleagues of our upcoming time off. But when it comes to Automatic Replies for out-of-office periods, who needs to know when we're gone and how much information do they really need?

In the context of cybersecurity, social engineering relies on human behavior to obtain information that could be leveraged to facilitate a cyber attack against us or our colleagues that could ultimately be used to commit fraud against or, otherwise, harm organizations. Something as seemingly innocuous as an Automatic (Out-of-Office) Reply could instantly provide attackers with valuable information. Malicious actors armed with the confirmation and information provided in OOO's can then craft very convincing social engineering attacks such as business email compromise (BEC) attempts with requests like diversion of payroll direct deposits (an attacker's favorite when we are out-of-office), fake invoice payments, and wire transfer account changes.

✓ **Automatic Replies erase doubt.** Scammers frequently send emails in bulk as an attempt to trigger OOO's for reconnaissance during customary seasons of known out-of-office time like vacations and holidays.
✓ **Automatic Replies can be a goldmine of information for scammers.** Out-of-Office replies often include details like the timeframe/duration away from work, alternate contacts that can be reached during the absence, the reason or location of the trip, and usually a customary email signature.
✓ **Automatic Replies are telling.** Out-of-Office replies confirm valid email addresses, the email address convention used at the organization, and sometimes the chain-of-command.

Enjoying time away doesn't have to be stressful. Planning ahead of time can alleviate some of the worries. Consider setting up one automatic reply message for external senders (even for pre-existing contacts) that excludes sensitive information, and another for internal senders that's more detailed. For example, external senders may only need to know that you are unavailable, and your response may be delayed, especially if they have not been advised beforehand.

FB-ISAO Advisory Board

[Get to Know the Board of Advisors]

Contact Us

Company Name
FB-ISAO

Email
Info@faithbased-isao.org

Website
www.faithbased-isao.org

Not Yet a Member of FB-ISAO?

How to join…

Not Yet on FB-ISAO Slack? You Need to Be!

Write to membership

Upcoming FB-ISAO Events

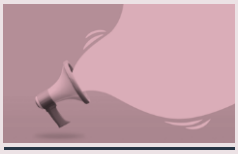
Office Hours. *(Meeting Invitations sent to all members via email.)*	27 June at 1:00pm ET
Coaching Session: How We Can Make a Difference	21 June at 2:00pm ET
2023 Educational Series: A Culture of Security	Monthly, the first Wednesday of each month at 12:00pm ET
AMA with Robert Goldberg	➤ 13 July ➤ 17 August ➤ 14 Sept. ***(All Sessions at 12:00pm ET)***

DBIR Anyone?

The Verizon's 2023 Data Breach Investigations Report is affectionately known as the "DBIR". The DBIR looks at the *"sordid underbelly of cybercrime"* to discern lessons everyone can learn from and prioritize our collective cyber defenses.

FB-ISAO members may find value in the *Small and Medium business* (SMB) section of the DBIR (beginning on page 65), as it provides glimpses across small organizations with less than 1,000 employees. While this section found that both small and large organizations are using similar technology services and infrastructure, most SMBs are not as prepared to respond to the cyber threats and attacks. Below are some notables from the DBIR. The list can be used to help organizations prepare for what the DBIR highlights as the most prevalent attack vectors.

➤ Social engineering and the human element reign supreme in factors resulting in confirmed breaches.
➤ Unsurprisingly, ransomware remains a reliable attack across all organizations.
➤ Also unsurprisingly, financially motivated organized crime tops the threat actor motives and categories in confirmed breaches.
➤ Despite media coverage, the average organization is more likely to be impacted by internal actors than state-sponsored actors.



Spotlight: Priority Intelligence Requirements

The FB-ISAO Communications Working Group is performing its annual review of the FB-ISAO Priority Intelligence Requirements (PIR). The PIR and corresponding Intelligence Requirements (IR) have been developed to inform both FB-ISAO staff efforts and to inform partners who may provide intelligence and information to FB-ISAO. PIRs are those concerns that are most critical to FB-ISAO, and IRs are general concerns relating to the all-hazards threat environment. The items identified in the PIR document are not to suggest exclusion of other relevant threat awareness information, SARs, or products from being shared with FB-ISAO. The PIR and IR include information in the following categories:

➤ Physical Security Threats.
➤ Cybersecurity Threats.
➤ Other Fraud and Other Criminal Threats.
➤ Public Health and Environmental Threats.

A PIR Explainer has been developed and posted here.

Do you want to contribute to the review? Join the Communications Working Group by writing to membership@faithbased-isao.org.