第1回経営者向け研修 Q&A

令和5年1月24日に開催いたしました第1回経営者向け研修におけるQ＆Aについて、下記通り回答いたします。

#	質問	回答
1	2つの病院が攻撃された日が「10月31日」というのは偶然の一致なのでしょうか。なにか思い当たる事項があれば、ご教示お願いします。	10月31日の一致は偶然ではないかと思います。 ・それ以外の日付でもランサムウェアのインシデントが起きている点 ・攻撃者グループが半田はLockbit、急性期はPhobosと異なることから
2	半田病院では復旧のために暗号化鍵の費用を払ったということも一部で言われていますが、そういった機関と交渉するような窓口もあったりするのでしょうか？	交渉を行ったことがあるといったベンダーがいるということは伺ったことがありますが、攻撃者とコンタクトするのは基本的に行いません。
3	ランサムウェアに攻撃されたときに交渉してはいけない、ということはよく理解できますが、その結果盗まれた個人情報が公開される危険はないのでしょうか？もし公開されたらどのように対応をするのでしょうか。膨大な要配慮個人情報が公開されることになりますが…	情報が漏洩してしまった場合、基本的に取り戻すことができず、アンダーグランドでどのような取引が行われるのかわかりません。基本的には法執行機関と連携し、対処に当たる他ありません。組織としてはどのようなデータが漏洩しているのか。本物であるのか保有するファイルのハッシュと照合し、漏洩したものか確認しておく位でしょう。
4	オンライン資格確認や電子処方箋の運用開始で各病院がよりセキュリティに対して真摯に取り組まないといけない状況になっていますが、ここを確認するべき運用としてこうするべきというのはあるのでしょうか。各病院まかせになってしまっているのではないでしょうか。	侵入経路となりうるポイントをまずは徹底的に見ることだと思います。外部との接続ポイントは、セキュリティ製品やログが取得出来ているのか、ネットワークの常時接続になっていないか。不用意にポートやプロトコルを許可していないかなど、できる設定から始めることかと思います。また脆弱性がある環境を無くす、既存のセキュリティ対策をより高い設定に変更する、ADのグループポリシーを徹底するなど、実施できるポイントはたくさんあると思われます。
5	外部事業者にセキュリティー確保のためのファームアップ等を確実に実施させるための効果的な仕様や、契約内容の書き方（標準的な記載方法）を教えてください。	例示：導入している製品やシステム、機器などのソフトウェアは、常に最新のバージョンやトラブル情報などを収集し、ソフトウェア更新がある場合は、病院に通知、協議の上、アップデートを行うこと。なお、ファームウェアの更新によりログが消去されてしまうため、Syslogを取得、ログの管理も適切に行うこと。
6	契約（保守）内容に「セキュリティパッチ対応等」を記載できるケースはどの程度あるのでしょうか。具体的には、大手電子カルテベンダーで対応している医療機関はありますでしょうか。多くの医療機関では断れらたとの声がたくさんありますが、現実として実績があるのでしょうか。契約に含めることは大切だと思いますが、いかがでしょうか？	別途仕様で定め、セキュリティ保守をどのように行うのか具体的に記載していく必要があります。現行の医療機関ではほとんどないと思われます。これまでは電カルの仕様やシステム・ネットワークの設計思想が古いにもかかわらず、変更に関る対応に工数・費用がかかるため、端的に拒んできた背景があると思います。厚生労働省の医療機器更新に関する通達、昨今のインシデントを受けて社会通念上、断るということがより難しくなってきていると思います。再度交渉を行うなどのご辛抱も頂きたいと思います。なお、大阪急性期総合医療センターがまさしくインシデント発生後、電カル、部門、機器ベンダーが真摯に向き合い更新対応などを多くのベンダーで対応頂いております。
7	説明している内容は理解できるが厚労省がこれをベースに物を考えると現場が回らない。現実離れしている部分が多い気がする。そもそもベンダーはこれを理解、対応しているのか？ベンダーを指導するほうが効果的ではないか？厚労省が現場に圧力をかけるだけになっていないか？	まずはできることから始めるという視点、どのようなインシデントが起きているのか共有し合うというところから始まっており、ベンダーとの向き合い方を考えるうえでもまずは医療機関に限定しています。病院も責任感をより一層強く持つこと、ご指摘の通り、ベンダーの意識が高まっていかないと解決していかない部分も多く、ベンダー任せではなく医療機関全体でベンダーの底上げを行っていくことも必要であると考えています。
8	厚労省へ通報をすると、どんなことをしてもらえるのか。調査に非常に時間がかかったりしないか？	初動対応支援を行える体制があります。大阪急性期総合医療センターはインシデント発覚当日に通報を行い、初日から政府派遣チームとして対応に当たっています。
9	サイバー攻撃を受けながら公表(会見)されていない事件もあるのでしょうか。あるとすれば、どのような事例で、どのように対処したのか教えてください。	お客様や関係者、二次被害が生じないなどというケースは公表されていないケース、また意図的に公表を行わなかったケースもあります。しかしながら、昨今ではSNSの浸透や改正個情報など、全く公開しないという選択肢はなくなってきているように思われます。過去にはお問い合わせがあれば回答する、最終報告書だけ公表するなど、様々な事例があります。
10	情報資産を確認するというのは、もう少し具体的にどうすれがいいのですか	端末・サーバ、USBやプリンタ、ネットワーク、データなど組織の情報を棚卸し、情報資産管理台帳を作って管理運用するということです。https://www.ipa.go.jp/files/000055518.xlsx
11	保守契約書には具体的にどのような文言を入れたらよいのでしょうか。	セキュリティ条項や監査条項を適切に盛り込む。脆弱性やソフトウェア更新などの対応はどのように行うのか仕様書に盛り込むことが必要ではないかと思います。セキュリティ条項はインシデントが発生した際に調査や連携協力を求める内容などの記載が必要です。
12	インシデントという言葉を多様されていましたが、アクシデントではないのでしょうか？インシデントというのは重大な事故につながりかねないリスクあることですが、今日講師が話されていたことはすべてアクシデント＝重大事故ではないのでしょうか？	医療用語と若干、異なる使い方をしています。サイバーセキュリティではインシデントにアクシデントも含まれて使われているケースが多く、アクシデントは重大インシデントといったような言い方を行う場合もあります。
13	こうした研修は質疑に十分な時間をとっていただいくことが各医療機関の何よりの対策になります。今後宜しくお願い致します。	来年度以降、時間配分を考えて研修実施を検討いたします。
14	バックアップについて、何セットとるか、また複数のシステムで取った方がよいのか、など、何か推奨されることがあれば教えてください。	代表的なバックアップのルールとしては3-2-1ルールがあります。 https://xtech.nikkei.com/atcl/nxt/column/18/01584/030500001/
15	復旧の優先順位を各病院で検討しておくとのことですが、病院としての最低限の機能を維持する上でどこでも優先順位は大体一緒になるのではと思うのですが、実際被害にあった2病院ではどのシステムから復旧させたのでしょうか？	画像関係や地域連携、医薬品調剤、診察券発行機など、患者の方が来られた際に迷惑とならぬよう、通常診療に必要な部分を優先的に対応を行っていたと思われます。
16	医療装置(放射線装置や検査機器)までランサムウェアの攻撃はおよぶのでしょうか	汎用的なOSが用いられている機器も多く、影響を受ける可能性があります。 https://softwareisac.jp/wp/?p=19936
17	基本的にシステムベンダーとは電子カルテ業者の事でしょうか？あまり本日の様な話をしたことはなく、オンプレだからなのか、業者は来てくれなくて、ほとんど自力で解決してく	原稿の保守や運用、導入時の契約などをまずはご確認頂くのがよろしいかと思います。電子カルテシステムベンダー、部門システムベンダー、ネットワークインテグレーター、システムインテグレーター、セキュリティベンダーなど、べんだーも様々です。
18	オフラインバックアップは何日分あるべきか？	医療継続に必要な日数というのが回答になります。頻度が高いことに越したことはないですが、費用との兼ね合いでの判断になると思います。
19	情報システムや医療機器のソフトウェアの脆弱性はどこから入手できるのでしょうか。	脆弱性を突く攻撃や新たなマルウェアなどの観点で言えば、ダークウェブやディープウェブ上から取得が可能です。
20	病院のランサムウェアの実被害、情報漏洩は何件ありますか。	ニュースサイトなどでご確認頂くと、複数件あることが確認できます。 https://scan.netsecurity.ne.jp/pages/search.html?q=%E7%97%85%E9%99%A2
21	インシデントがアクシデントも含む言葉として使用されているように見えるのは、気になりました。インシデントの時点で、厚生労働省へ連絡をすれば、何かしらの示唆をいただけるということでしょうか？	サイバー攻撃におけるインシデントはアクシデントを含まれて使われる傾向が強く、イベント（インシデント事象）というインシデントの可能性と使い分けて用いられています。インシデントはご連絡頂ければ、状況に応じ初動対応のご支援などが行えると思います。
22	バックアップデータのオフライン保存は既にしています。オンライン保存は必須でしょうか	医療の継続に支障をきたさない場合はオフラインだけでも構わないとはお思いますが、データや構成情報など、様々なバックアップが必要ではないかと思います。一般的には3-2-1ルールというバックアップを取得するというのが教科書的な回答です。 https://xtech.nikkei.com/atcl/nxt/column/18/01584/030500001/
23	セキュリティ対策に関する補助金、助成金などの制度があれば教えてください。	現在、あるのは経済産業省が実施しているIT補助金が対象になろうかと思います。
24	実際の復旧手順をご教授お願い致します。	状況によって異なりますが、まずはデータの保全を行い、フォレンジックなどの詳細調査を行い、結果を待って戻すというのが最適です。しかしながら、全てをフォレンジックするのも現実出来はありません。初期化が可能であれば初期化を早々に行うというのも一つですが、原因がわからないため再度感染する可能性も否定できません。 その他にも侵害を確認できるツールを用いて調査を行う、他のウイルスが侵入していないファイルをセキュリティベンダーに解析してもらい、新しいマルウェアがあった場合は、パターンファイルが作成された後にフルスキャンを行って戻すなど、感染状況によって対応が異なります。