Secureworks

CASE STUDY

業種を問わず重要なサイバーセキュリティ対策も航空会社にサービスやデータを提供・共有する企業では「必須条件」に

業種：航空

国：米国

業務への影響

- 収益
- コスト最適化
- 生産性
- 業務効率

米州3か国に4施設を要する世界有数の航空機部品メーカーがあります。同社は、航空業界最大手の企業数社を顧客に有し、信頼のおけるパートナーとしてサービスを提供しています。

同社には一流の技術者が揃っており、世界最高水準の安全性と品質を提供しています。しかし航空機の運航は人命にかかわることであり、サイバー脅威は機械の故障と同等に深刻な問題であることから、「機械の完全生」だけでなく「データセキュリティ」についても同様に保証するよう、顧客から求められています。

同社は複数企業の合併によって誕生したため、いくつか乗り越えるべき課題がありました。具体的には、個別のセキュリティシステムを単一プログラムに統合すること、3ヵ国にまたがる複数拠点をカバーすること、場合によっては地域固有のリスクに対処することが必要でした。

サイバー攻撃が増加するなか、もし被害に遭った場合は収益、事業機会、評判、ISO認証のすべてが危機に瀕することを同社経営陣は理解していましたが、自社のセキュリティニーズを充分に満たせる規模の社内チームを発足させるには時間とコストがかかりすぎることも理解していました。そこで、ニーズにマッチする外部委託先を複数検討した結果、Secureworksが最適であるという結論に達しました。

「ランサムウェア攻撃からの復旧コストについて経営陣からたずねられた際、年間3～4回発生すると仮定して1件あたり200万ドル程度になるだろう、と回答しました」

「この総額はランサムウェアによる被害だけでなく事業損失も含んでいます。前職でハッキング被害が発生した際は、6週間にわたってシステムがダウンしました。現在の勤務先では75本の生産ラインが稼働しており、同様のインシデントが起これば毎週何百万ドルものコストが発生する恐れがあります」

IT リスク・コンプライアンス
マネージャー

お客様が抱えていた重要なビジネス課題

- サイバーセキュリティに関するすべてのオペレーションの水準を引き上げ、自社および顧客のデータを保護すること
- 生産ラインが停止に陥るようなセキュリティ侵害から自社を保護し、事業の継続性を維持すること
- ISO認証を取得し、有益な契約を獲得・維持すること
- 以下を活用し、セキュリティ投資の価値を最大化すること：
  - 最新のセキュリティソフトおよび専門知識（24時間365日体制のサポート含む）
  - 継続的な脅威動向の追跡管理および、潜在的な侵害に関するリアルタイムレポート
  - 必要な社内セキュリティ専門チームの規模を適正化

Secureworksの導入効果

合併による事業成長は常に課題を伴います。異なるシステムや組織文化を融合させるには時間と忍耐が必要です。しかし同社は、航空産業の大手顧客から信頼される製造パートナーとして一刻も早く全社的なセキュリティ態勢を強化する必要がありました。

全社的なセキュリティ態勢を最高水準に引き上げることは大変な作業でした。IT成熟度は取引先によって異なり、ほぼすべて紙ベースのシステムを使っている企業もありました。また、1万人もの社員が3カ国にまたがる各拠点に在籍しているため、多様な人員の地理的な分散という問題に加えて、地域特有の問題もありました。

同社では複数のセキュリティ領域に脆弱性があり、経営陣も当該リスクを把握していました。サイバー攻撃が一度でも発生すれば何百万ドルもの収益や事業機会を失うだけでなく、信頼される企業としての「評判」も失墜します。強固なセキュリティプログラムなくしてISO認証は取得できません。ISO認証がなければ、獲得可能な顧客層が狭まるため事業機会が制限され、保険コストもかさみます。

専門家の支援が必要なことは経営陣も認識していましたが、優秀なセキュリティ人材は引く手あまたであり、一部地域では新規採用や人材維持がほぼ不可能な状態だったため、社内チームを短期間で発足させることは到底できませんでした。そこで外部ソリューションに着目し、複数のベンダーから提案を取り寄せた結果、セキュリティパートナーとしてSecureworksを採用しました。

同社はSecureworksとの協業により、24時間体制での脅威の追跡管理および防御対策を含む堅牢なセキュリティプログラムを短期間で整備することができました。現在は、Secureworksと共にセキュリティ態勢全般をさらに強化するための社内チーム発足に向け、優秀な人材を育成する時間的余裕も生まれ、社員1万人規模の組織全体をランサムウェア、セキュリティ侵害、サイバー攻撃から保護できています。同社のITリスク・コンプライアンスマネージャーは、こうしたセキュリティ保護による節減効果を以下のとおり見積もっています。

「現職では、1日平均6件のセキュリティイベントに対処していますが、侵害に発展する恐れがあるインシデントに分類されるのはそのうち3件ほどです。侵害が発生すると1件あたり約5万ドルのコストがかかります」

「ISO認証を取得すれば、保険コストだけでも毎年5～10%は節減できるでしょう」

「お客様にとっては、当社のシステムやセキュリティが頼りです。ISO認証があれば、最大6%の増収が見込めるほか、認証効果によって新規契約を増やせます。当社は重要なサプライチェーンの一角を成していますが、変化するセキュリティ環境のもと、サプライチェーンにおけるISO認証の必要性は明らかです」

ITリスク・コンプライアンス
マネージャー

ランサムウェア対策

年間600万ドル（攻撃の発生件数：毎年3件、1件あたりの対応コストを200万ドルと控えめに仮定した場合）

侵害対策

年間180万ドル（インシデント発生件数：毎月3件、月単位の対応コストを15万ドルと仮定）

サイバー攻撃対策

週換算利益で200万ドル（サイバー攻撃1件で75本の生産ラインが停止すると仮定）

セキュリティレベルの強化

時間換算収益で30万ドル（業務オペレーション中断の防止により）

チームの規模

社内チームは6名体制の予定だが、Secureworksとの協業がなければ、少なくとも倍の規模が必要

同社のITリスク・コンプライアンスマネージャーは、Secureworksとの協業窓口として、6名構成のスリムな社内チームを発足させるべく取り組んでいます。実践能力に長けたSecureworksの専門家の支援を得られるため、社内チームのメンバーは若手1～2名、中堅数名、ITセキュリティ管理者1名、上席専門家1名で充分対応できる予定です。「Secureworksの支援がなければどの程度の人員が部内で必要になっていたのか、想像もつきません。少なくともこの倍は必要だったでしょう」と同氏は述べています。

セキュリティ専門の有資格者に対する需要はかつてないほど高まっており、人材の採用・維持が困難なことは周知の事実です。地域によっては、必要な専門知識を備えた人材を見つけることすらできないため、採用後にOJTを通じて教育しなければなりません。会社が求めるセキュリティ保護をSecureworksが提供することで、前述のITリスク・コンプライアンスマネージャーは「今日のリスク緩和に必要な対策」だけでなく、「強固な社内チームづくりに必要な時間的余裕」も得られます。

前述のマネージャーによると、社内チームが発足してセキュリティ態勢が強化されると「新規事業の獲得により、5～6%の増収機会が見込める」とのことです。さらにISO認証の申請も可能になります。これにより、保険料が5～10%削減できる一方、事業機会が拡大します。同社は過去に、ISO認証を取得していないという理由で300万～500万ドル規模の契約を1件失注していたこともあり、認証取得による効果をよく理解しています。

「Secureworksを最大限活用しただけで、セキュリティ対策の水準がレベル1からレベル4に改善しました。他のセキュリティ機能についてもSecureworksへの統合を進めていますが、これまでに比べて状況認識の精度も高まりました。Secureworksがインシデントを隔離してくれるおかげで1時間あたり30万ドルのコストを節減でき、75本の生産ラインを止めずに操業できます」

「セキュリティ侵害を受けると、コスト面で甚大な影響が及びます。システムが停止すると、システム利用料金は減りますが、費用は上昇する一方です。当社の経営陣は、業務を止めないことによる価値、およびランサムウェアなどから常に自社を守ることの価値を実感しています」

「今日の脅威環境は、悪意あるコードが埋め込まれたパソコン用USBメモリと同じぐらい単純かもしれません。当社は3ヵ国に6つの拠点を展開しています。環境的な要素はコントロールできませんが、自らコントロールできる領域はしっかり統制しなければなりません。つまり、今日の企業が直面するサイバー犯罪やランサムウェア、セキュリティ脅威から適切に身を守る、ということです」

ITリスク・コンプライアンスマネージャー

Secureworks®

同社にとって、自社の防御対策強化、社内データの保護、顧客が求める世界水準のサイバーセキュリティの実現に必要なセキュリティパートナーはまさにSecureworksでした。

測定指標

600万ドル ランサムウェア攻撃対策により、**年間600万ドルの節減効果を想定**（攻撃発生件数：年間3件、1件あたりの対応コスト：200万ドルと控えめに試算）

180万ドル 侵害対策により、**年間180万ドルの節減効果を想定**（インシデント発生件数：月3件程度、1件あたりの財務的影響額：5万ドル＝月換算15万ドルで試算）

200万ドル サイバー攻撃対策により、**週換算で最大200万ドルの利益を保護**（攻撃を受けた場合、75本の生産ラインが数週間停止すると仮定）

30万ドル **社内セキュリティレベルの抜本的強化**（生産ラインの中断を防止できれば、時間換算で30万ドル程度の収益を逸失せずに済むため）

50万ドル 6名体制のスリムな社内セキュリティチームで3カ国6拠点を保護：Secureworksを導入しなかった場合、さらに6名の増員が必要となっていたため、**少なくとも年間50万ドルの節減効果**が見込める（新規採用、教育、人材維持に関する大々的投資が不要となるため）

将来的なメリット

- セキュリティ態勢強化により新規顧客への拡販が進むことで、5～6%程度の潜在的増収効果が見込める
- ISO認証取得の確度が高まることで、新規事業の機会がさらに拡大（直近の実績をもとに、契約1件あたり300万～500万ドルと試算）
- 保険コストを5～10%低減できる見込み

「セキュリティソリューションの検討にあたり、複数のベンダーに提案を依頼しましたが、最終的に当社の求める姿を最適な形で支援してくれるのはSecureworksでした」

「全体で1万人の社員がいますが、従業員数が多ければリスクも高いことは承知しています。そこで、セキュリティソリューションの選定においてもこの点を考慮しました」

「Secureworksの支援があれば、ITリスク・コンプライアンス部は実際の規模以上の力を発揮できます。Secureworksのソリューションによって、セキュリティ対策効果が倍増しました。Secureworksの人材およびサービスは我々の日常業務に大変役立っています」

ITリスク・コンプライアンスマネージャー

詳細は、当社のセキュリティスペシャリストにご相談ください。
☎03-4400-9373
secureworks.jp